CYBERWAR AND B.H. LIDDELL HART'S INDIRECT APPROACH

A thesis presented to the Faculty of the U.S. Army
Command and General Staff College in partial
fulfillment of the requirements for the
degree

MASTER OF MILITARY ART AND SCIENCE
General Studies

by

BRANDON THOMAS EUHUS, LIEUTENANT, U.S. NAVY
B.A., University of Oklahoma, Norman, Oklahoma, 2010

Fort Leavenworth, Kansas
2016

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE *(DD-MM-YYYY)* 10-06-2016	**2. REPORT TYPE** Master’s Thesis	**3. DATES COVERED** *(From - To)* AUG 2015 – JUN 2016

4. TITLE AND SUBTITLE Cyberwar and B.H. Liddell Hart’s Indirect Approach	**5a. CONTRACT NUMBER**
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) LT Brandon T. Euhus, USN	**5d. PROJECT NUMBER**
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) U.S. Army Command and General Staff College ATTN: ATZL-SWD-GD Fort Leavenworth, KS 66027-2301	**8. PERFORMING ORG REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)	**10. SPONSOR/MONITOR’S ACRONYM(S)**
	11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This study attempts to illuminate cyberwarfare’s efficacy as an indirect approach using B.H Liddell Hart’s principles of the indirect approach as described in his book, *Strategy*. His principles are applied to two well-documented cyber attacks. The first is Stuxnet, which refers to the 2010 U.S.-Israeli cyber operation targeting Iran’s nuclear program. The second deals with advanced persistent threats stemming from Chinese cyber espionage. Each attack profile, while sharing a common maneuver domain (cyber), employs distinctive methods in pursuit of different objectives. Stuxnet was purpose built to infiltrate and destroy specific nuclear centrifuges within Iran. Conversely, Chinese cyber espionage is designed to extract massive amounts of data over a period of months and years. This dichotomy provides sufficient breadth in the application of Liddell Hart’s principles. The purpose is to evaluate the efficacy of B.H Liddell Hart’s principles to cyberwar and gain a deeper understanding of how conflict in cyberspace translates to other domains and across the levels of war. Additionally, the study seeks to answer the following questions. Is cyberwarfare an indirect approach by its very nature? What does an indirect cyber approach look like? Can cyberwarfare achieve decisive results when used as an “indirect approach?”

15. SUBJECT TERMS

B.H. Liddell Hart, Cyberwar, Iran, Stuxnet, China, Cuber Espionage

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT (U)	**b. ABSTRACT** (U)	**c. THIS PAGE** (U)	(U)	158	**19b. PHONE NUMBER** *(include area code)*

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

Name of Candidate: LT Brandon T. Euhus

Thesis Title: Cyberwar and B.H. Liddell Hart's Indirect Approach

Approved by:

______________________________________, Thesis Committee Chair
John T. Kuehn, Ph.D.

______________________________________, Member
Sean N. Kalic, Ph.D.

______________________________________, Member
Brian J. Gerling, M.S.

Accepted this 10th day of June 2016 by:

______________________________________, Director, Graduate Degree Programs
Robert F. Baumann, Ph.D.

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other governmental agency. (References to this study should include the foregoing statement.)

ABSTRACT

CYBERWAR AND B.H. LIDDELL HART'S INDIRECT APPROACH, by LT Brandon T. Euhus, 158 pages.

This study attempts to illuminate cyberwarfare's efficacy as an indirect approach using B.H Liddell Hart's principles of the indirect approach as described in his book, *Strategy*. His principles are applied to two well-documented cyber attacks. The first is Stuxnet, which refers to the 2010 U.S.-Israeli cyber operation targeting Iran's nuclear program. The second deals with advanced persistent threats stemming from Chinese cyber espionage. Each attack profile, while sharing a common maneuver domain (cyber), employs distinctive methods in pursuit of different objectives. Stuxnet was purpose built to infiltrate and destroy specific nuclear centrifuges within Iran. Conversely, Chinese cyber espionage is designed to extract massive amounts of data over a period of months and years. This dichotomy provides sufficient breadth in the application of Liddell Hart's principles. The purpose is to evaluate the efficacy of B.H Liddell Hart's principles to cyberwar and gain a deeper understanding of how conflict in cyberspace translates to other domains and across the levels of war. Additionally, the study seeks to answer the following questions. Is cyberwarfare an indirect approach by its very nature? What does an indirect cyber approach look like? Can cyberwarfare achieve decisive results when used as an "indirect approach?"

ACKNOWLEDGMENTS

I would like to thank Staff Group 14A for a year of camaraderie and intellectual stimulation; iron sharpens iron. I am also indebted to Dr. Jack Kem for his total commitment to my personal and professional growth. Through his instruction I learned conceptual and detailed planning, and, I think, how to distinguish between the two. In addition, by his example, I gleaned the skills required to be a more professional military officer. I would like to thank Mr. Bill Knight for truly looking out for the welfare of our entire staff group.

I am grateful for the excellent guidance I received throughout this year from my MMAS committee. I am especially thankful to Dr. John Kuehn for his willingness to guide me from start to finish as the committee chair. He was instrumental to the success of this project and continuously encouraged me to push the pace and “do more.” Dr. Sean Kalic provided valuable expertise and critiques, and Mr. Brian Gerling provided expert guidance on cyber issues. Thank you for your steady support.

Finally, I would like to thank all my kids for their encouragement and support throughout this year. I absolutely cherish the nights we spent working together on our homework. I especially want to thank my wife. She is the unshakable foundation of our family and I love her with all of my heart.

TABLE OF CONTENTS

Page

ACRONYMS

APT	Advanced Persistent Threat
CAM	Combined Arms Maneuver
CCP	Chinese Communist Party
DDoS	Distributed Denial of Service
DoD	Department of Defense
IAEA	International Atomic Energy Agency
INEW	Integrated Network Electronic Warfare
IP	Intellectual Property
LH	Basil Henry Liddell Hart
NIE	National Intelligence Estimate
OPM	Office of Personnel Management
PLA	People’s Liberation Army
PLC	Programmable Logic Controller
PRC	People’s Republic of China
RMA	Revolution in Military Affairs
SCADA	Supervisory Control and Data Acquisition
WWI	World War I
WWII	World War II

ILLUSTRATIONS

Page

CHAPTER 1

INTRODUCTION

In January 2010, news outlets reported that Google was the victim of a deliberate cyber attack resulting in the extraction of intellectual property (IP) that included valuable source code. The attack, known as Operation Aurora, was notable due to its complexity and the type of information extracted. This indicated the attack was state sponsored and not the work of a rogue hacker. The subsequent investigation linked the attack to China.[1]

In March of 2013, President Barack Obama called on China to cease the relentless cyber attacks targeting U.S. companies and government agencies.[2] However, intrusions continued unabated. Furthermore, in June 2015, U.S. officials acknowledged hackers penetrated networks belonging to the Office of Personnel Management and that information extracted compromised the personal data of four million people.[3] By September the number affected increased to 21.5 million with the vast majority wholly

[1] Kim Zetter, "Google Attack Was Ultra Sophisticated, New Details Show," *Wired*, 14 January 2010), accessed 7 September 2015, http://www.wired.com/2010/01/operation-aurora/.

[2] Ellen Nakashima, "US Publicly Calls on China to Stop Commercial Cyber-Espionage, Theft of Trade Secrets," *The Washington Post*, 11 March 2013, accessed 7 September 2015, https://www.washingtonpost.com/world/national-security/us-publicly-calls-on-china-to-stop-commercial-cyber-espionage-theft-of-trade-secrets/2013/03/11/28b21d12-8a82-11e2-a051-6810d606108d_story.html.

[3] Ellen Nakashima, "Chinese Breach Data of 4 Million Federal Workers," *Washington Post*, 4 June 2015, accessed 7 September 2015, https://www.washingtonpost.com/world/national-security/chinese-hackers-breach-federal-governments-personnel-office/2015/06/04/889c0e52-0af7-11e5-95fd-d580f1c5d44e_story.html.

unaware.[4] "U.S. officials said the breaches rank among the most potentially damaging cyber heists in U.S. government history because of the abundant detail in the files."[5] The data extracted included millions of SF-86's, which are the biographical information forms used to initiate federal background checks for awarding security clearances. The forms contain multitudes of personal and sensitive information, not just about the individual but also data associated with spouses, immediate family members, and employers. The information contained in a SF-86 is valuable to any foreign intelligence agency and can be used for blackmail or sold to identity thieves.[6] The severity of the OPM breach continues to unfold. In response, OPM "awarded a $133 million contract in an effort to provide credit monitoring services for three years to nearly 22 million people."[7] In response the Obama Administration threatened to enact economic sanctions aimed at specific individuals and businesses affiliated with the Chinese Government.[8] Ultimately,

[4] Chris Brooks, "Victims of June OPM Hack Still Haven't Been Notified," *Threat Post,* 2 September 2015, accessed 7 September 2015, https://threatpost.com/victims-of-june-opm-hack-still-havent-been-notified/114512/.

[5] Ellen Nakashima, "Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say," *Washington Post,* 9 July 2015, accessed 7 September 2015, http://www.washingtonpost.com/blogs/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/.

[6] Kim Zetter and Any Greenberg, "Why the OPM Breach is Such a Security and Privacy Debacle," *Wired,* 11 June 2015, accessed 7 September 2015, http://www.wired.com/2015/06/opm-breach-security-privacy-debacle/.

[7] Brian Krebs, "OPM (mis)Spends $133M on Credit Monitoring," Krebs on Security, 2 September 2015, accessed 7 September 2015, http://krebsonsecurity.com/2015/09/opm-misspends-133m-on-credit-monitoring/.

[8] John Zorabedian, "Should the US hit China with Sanctions over Cyber-Espionage?" *Naked Security,* 3 September 2015, accessed 7 September 2015, https://nakedsecurity.sophos.com/2015/09/03/should-the-us-hit-china-with-sanctions-over-cyberespionage/?utm_source=Naked%2520Security%2520-%2520Feed&utm_

the United States backed away from the proposal, which would have marked the first instance the president relied on economic sanctions to counter cyber espionage since the Congress granted the executive order approval on 1 April 2015.

Western countries consider access to information a fundamental right. This perspective informs the way Western governments and their citizens' perceive cyber issues. Arguably, authoritarian regimes consider information to be a weapon that can be wielded in order to censure and repress a populace and as a means to obtain valuable information on adversaries. It should be no surprise that the Chinese are waging a comprehensive cyber espionage campaign aimed at extracting IP and personal information.

States acknowledge that espionage will occur. Arguably, the prevalence and perceived necessity buffers an unwanted escalation of force. In fact, "highly invasive, espionage does not constitute a use of force (or armed attack) under international law absent a nonconsensual physical penetration of the target's state territory."[9] Historically, cyber espionage does fit in the category of an "illegal" intelligence activity amongst states, despite data that suggests incessant cyber espionage costs companies upwards of $400 billion annually.[10]

medium=feed&utm_content=rss2&utm_campaign=Feed&utm_source=Naked+Security+-+Sophos+List&utm_campaign=77926f634f naked%252Bsecurity&utm_medium=email&utm_term=0_31623bb782-77926f634f-454898153.

[9] Catherine Theohary and John Rollins, *Cyberwarfare and Cyberterrorism: In Brief* (Washington, DC: Library of Congress, 27 March 2015), 6.

[10] Ellen Nakashima and Andrea Peterson, "Report: Cybercrime and Espionage Costs $445 billion annually," *The Washington Post,* 9 June 2014, accessed 7 October 2015, https://www.washingtonpost.com/world/national-security/report-cybercrime-and-

Espionage's cyber variant has exponentially increased the amount of information that can be stolen and reduced the risks of compromise due to issues with attribution. A lack of attribution also makes it difficult to determine motive and consequently to identify the authorizing agent (either a state government or non-state actor). Additionally, as seen in the OPM breach, cyber hacks have the ability to directly affect people not connected to the intelligence or defense community. In short, when compared with traditional forms of espionage the cyber variant is more visceral, cheap and gritty.

This study examines cyber warfare using principles of Basil Henry Liddell Hart's (LH) indirect approach in order to determine cyberwarfare's potential to achieve decisive results at the strategic level of war. Additionally, this study seeks to determine if cyberwarfare constitutes an indirect approach by its very nature. What does an indirect cyber approach look like? Can cyber warfare achieve decisive results when used as an "indirect approach?"

Primary Research Question

Does cyberwarfare constitute an indirect approach by its very nature; if not, what would an indirect approach look like in the cyber domain?

Secondary Research Questions

1. Can cyberwarfare achieve decisive results or contribute positively to a nation's strategic interests?

espionage-costs-445-billion-annually/2014/06/08/8995291c-ecce-11e3-9f5c-9075d5508f0a_story.html.

2. What is meant by cyberwarfare? In other words, has there been a cyberwar to date or only cyber attacks? Additionally, is the term cyberwarfare a misnomer?

3. How does the United States view the cyber domain? What is China’s view? Do divergent perspectives lead to tension?

4. What role does private industry play in shaping the ways and means of conflict in the cyber domain? Do they view the threats different than a sovereign state?

5. What role does the U.S. Department of Defense (DoD) play in the cyber domain? What capability gaps has DoD identified, if any, in order to maximize effectiveness in the cyber domain?

6. If the variable of attribution is solved, would it make it easier for governments to develop international norms regulating cyber conduct?

Significance

Cyber security expert and RAND researcher Martin Libicki in his book, *Conquest in Cyberspace: National Security and Information Warfare*, argues that any discussion on the relevance or applicability of the cyber domain in war is really just a rephrasing of the question, “Which medium dominates war?” He posits that the answer, regarding cyber, is “neither ‘yes’ or ‘no’ but ‘more so every day’.”[11]

Searching ‘cybersecurity’ through Google yields millions of results in less than one second. While this only indicates interest, the results highlight a variety of educational/job opportunities and relevant news articles. The number of threats

[11] Martin Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (New York: Cambridge University Press, 2007), 291.

potentially stemming from the cyber domain has outpaced the number of credentialed personnel capable of defending vulnerable networks. Globalization and advancements in communication infrastructure has allowed people worldwide, not just in developed countries, access to information. However, the cyber domain also allows governments, especially those in closed systems, to exploit vulnerabilities to maximize control. For these countries, the goal is not safeguarding information networks but controlling the information itself.

Consequently, the cyber domain is not only useful as a medium for communication but also for commerce, information storage, and controlling critical infrastructure. Arguably, the potential to conduct meaningful cyber attacks increases as nations and citizens continue to demand uninterrupted access to digital information. Additionally, as companies continue to develop and implant increasingly complex technology into user-friendly devices consumers continue to overlook the myriad methods available to exploit their devices. It is not just a lack of cyber education that is problematic but also an appreciation for an adversary's ends, ways, and means in cyberspace. A recent news article highlighted that within the U.S. National Security Agency there is "an invisible war of lawyers arguing over what counts as a cyber operation."[12] The United States commands an impressive repertoire of cyber capabilities but rules of engagement lag behind. Also of concern is the ongoing cyber espionage campaign affecting U.S. private and public industries. The recent establishment of U.S.

[12] Kelly McEvers, "Rules for Cyberwarfare Still Unclear, Even as US Engages in It," *NPR*, 20 April 2016, accessed 27 April 2016, http://www.npr.org/templates/transcript/transcript.php?storyID=475005923.

Cyber Command in 2010 as a sub-unified command under U.S. Strategic Command acknowledges the importance of the cyber domain to national security.

However, the United States owns no monopoly on cyber operations. For example, nations such as China, Russia, Iran, and India have aggressively taken steps to strengthen their cyber preeminence, as have various non-state actors, criminal organizations, and loosely affiliated groups.[13] Each of these entities has demonstrated the capacity to conduct meaningful cyber attacks. Additionally, the private sector owns, develops, and controls significant elements of cyberspace. The true litmus test for cyber will be demonstrating the ability to achieve decisive results and validating that operations across the cyber domain were crucial for overall success. Currently, the majority of military professionals focus their training on combat operations within the traditional domains of air, land, and sea and have an acute understanding of conventional capabilities, mission planning, and the ways to achieve the military end state.[14] Cyber experts understand computer science, network architecture, and vulnerabilities in the cyber domain. In the future the rapid blurring of lines between the traditional professional military service member and a DoD affiliated cyber expert will challenge conventional norms. This requires military professionals to become aware of current and future cyber capabilities and their impacts on traditional military activities.

[13] Robert A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to do About It* (New York: HarperCollins, 2010), 147-149.

[14] Military professionals also rely heavily on space-based assets to conduct military operations, but historically, this is non-weaponized domain, restricting space-based operations to assist activities on air, land and sea. See Sean Kalic's, *US Presidents and the Militarization of Space, 1946-1947* (College Station: Texas A&M Press, 2012).

Assumptions

1. Cyber capabilities within the DoD are more concerned with defensive operations and network resiliency while offensive capabilities are developed and controlled by national intelligence agencies.
2. The complexity and sensitivity associated with operating in the cyber domain inhibits the incorporation/inclusion of cyber capabilities into traditional military mission sets. This is beginning to change incrementally as DoD builds its cyber capabilities.
3. Citizens will begin to demand that their government protect their cyber personas and information. A lack of effective protection may undermine the government's credibility.
4. The rise of non-state actors and loosely affiliated groups capable of conducting cyber attacks will be viewed as a direct threat against a government's monopoly on the use of force.

Literature Review

The literature review consists of two parts. The first part focuses on LH, his adherents, and critics. The second part will discuss the open source literature on cyberwarfare. LH's *Strategy* will provide the applicable narrative and the principles of the indirect approach.[15] Additional resources include Brian Bond's, *Liddell Hart: A Study of His Military Thought* and John J. Mearshiemer's, *Liddell Hart and the Weight of*

[15] The specific version is: B. H. Liddell Hart, *Strategy*, 2nd rev. ed. (New York: Meridian, 1991).

History. Both books discuss the evolution of LH's military theories and how his advocacy of maneuver warfare shifted from the end of World War One (WWI) through the end of World War Two (WWII).

Brian Bond originally published his book in 1977. Bond knew LH personally and credited him with launching his career as a military historian.[16] John Mearsheimer's book was published in 1988 and addresses Bond's critique directly while also contributing an original analysis of LH that chronologically charts LH's theories through time. This study acknowledges the evidence against LH but concludes that the principles of his indirect approach merit closer analysis.

The second part of the review discusses the open source cyber literature. The purpose is to place the cyber domain in a particular context, understand how this domain informs national security policy, and determine the potential impact on future military operations. A good source for survey level material on cyber security and cyber warfare is Peter W. Singer's and Allan Friedman's, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (2014). This book is written by known authorities on the subject and is on the Chief of Naval Operations reading list. Other sources include Martin Libicki's, *Conquest in Cyberspace: National Security and Information Warfare* (2007), which argues that friendly conquest of cyberspace may have more inherent benefits than hostile conquest. Jason Healy's, *Fierce Domain: Conflict in Cyberspace 1986-2012* (2013), looks at the history of cyber conflict.

[16] Brian Bond, *Liddell Hart: A Study of His Military Thought* (Aldershot, VT: Gregg Revivals, 1991), iii.

Research Design

Primary sources include the principles of the indirect approach found in LH's *Strategy* and sources that discuss Stuxnet and Chinese cyber espionage provide the framework for analysis. The purpose is to evaluate the efficacy of LH's principles to cyberwar and gain a deeper understanding of how actions in cyberspace translate to other domains and across levels of war. Secondary sources provide context and point to additional primary source materials.

Summary of Proposed Chapters 2-7

Chapter 2: Cyber Literature Review

This chapter reviews current open source literature on cyberwarfare. The purpose is to understand how various experts, across disciplines, discuss the cyber domain. Martin Libicki's, *Conquest in Cyberspace: National Security and Information Warfare* (2007), argues that the "Possibilities of hostile conquest may be less consequential than meets the eye while the possibilities of friendly conquest ought to be better appreciated."[17] *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World* (2012), edited by Derek Reveron, is a collection of scholarly articles divided into three parts: (1) Thinking About Cyber; (2) Armed Conflict and Cyber Defense; and(3) National Approaches to Cybersecurity and Cyberwar. Peter Singer's and Allan Freidman's book, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (2014), is a survey level book that orients the reader to the workings of the Internet and why cybersecurity is an issue. Cybersecurity professional Jason Healy, editor of *A Fierce*

[17] Libicki, *Conquest in Cyberspace,* 3.

Domain: Conflict in Cyberspace, 1986-2012 (2013), looks at the history of cyber conflict between 1986-2012.

Chapter 3: LH Literature Review

Brian Bond's, *Liddell Hart: A Study of His Military Thought* (1991), originally published in 1976, attempts to "Put Liddell Hart's military thought in proper perspective by tracing the origins and development of his principal ideas over his whole career."[18] The purpose of the book is not to silence criticism of LH, but to provide context and a medium to evaluate LH's arguments and objections based on primary source documents. John J. Mearsheimer's, *Liddell Hart and the Weight of History* (1988), reviews LH's writings/arguments/recommendations during the interwar period and directly following.

Chapter 4: Research Methodology

LH's strategy of the indirect approach from *Strategy* outlines eight principles.

Positive:

1. Adjust your end to your means - Learn to face the facts while still preserving faith.
2. Keep your object always in mind - Realize that there are more ways than one of gaining an objective.
3. Choose the line (or course) of least expectation - Think of what course the enemy will consider the least probable.

[18] Bond, 5.

4. Exploit the line of least resistance - “The longer the distance that has to be covered, the greater the ratio of natural obstacles, but the less the ration of opposition.”
5. Take a line of operation which offers alternative objectives - This shouldn’t be confused with pursuing a single objective. - Refers to putting the enemy of the “horns of a dilemma.”
6. Ensure that both the plan and dispositions are flexible – adaptable to circumstances - This refers to concentration and the ability to ensure elements/units can be mutually supportive. LH discusses the concept of concentration in greater detail and considers it a fundamental factor in success. For example, “True concentration is the fruit of calculated dispersion.”

Negative:

7. Do not throw your weight into a stroke whilst your opponent is on guard - No effective stroke is possible until his power of resistance or evasion is paralyzed.
8. Do not renew an attack along the same line (or in the same form) after it has once failed - You should assume the enemy will be even better prepared next time. [19]

[19] Liddell Hart, *Strategy*, 330-337.

Chapter 5 addresses the Stuxnet operation and applies the analysis discussed above. Chapter 6 addresses China-sponsored cyber espionage and applies the analysis discussed above.

Chapter 7: Conclusion

The conclusion will include a synthesis of the analysis. The goal will be to answer, “So what?” Can the cyber domain achieve, or at least contribute to, a decisive result? What is cyber’s potential? Are there any capability shortfalls or trends that may create a vulnerability that can be exploited by our adversaries to paralyze, dislocate, or mute U.S. ability to execute an effective response?

CHAPTER 2

CYBER 101 AND CYBERWAR LITERATURE

The current cyber literature provides analysis from a variety of perspectives. The breadth of scholarship makes it clear that experts across disciplines see value in studying the cyber domain and comprehending its efficacy and potential impacts on warfare and conflict in general. The literature focuses on analyzing cyber threats, especially cyber espionage and crime, in order to infer the implications at various levels (social, legal, political). Additionally, many scholars debate how cyber capabilities (offense and defense) may translate across the levels of war (strategic, operational, tactical) and the instruments of national power (diplomatic, information, military, economic). This breadth indicates two things. First, it shows that cyber's influence extends well beyond computer scientists, network architects, and those with a technical expertise. Second, it demonstrates the subject's lack of overall depth. Arguably, the current lack of depth is helpful because it facilitates a broader and more inclusive discussion. However, it also highlights that our understanding continues to take shape and that no nation or strategy has achieved clear predominance.

The underlining question the literature attempts to answer is, "So what?" Experts studying the cyber domain are particularly interested in understanding how activities in cyberspace reverberate across fields. The answer to this question depends on individual expertise and perspective. The pace of technological advancement, an insatiable reliance on network infrastructure, and a growing body of empirical evidence places the impetus on a careful and thoughtful analysis leading to new insights on the significance of cyber as an instrument of national power.

Cyber 101

Before discussing the current literature it is necessary to provide an overview on the cyber domain. The purpose is to gain a survey level understanding of the characteristics, key terms, and important issues. Joint Publication 3-12(R), *Cyberspace Operations* defines cyberspace as, "A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[20]

The definition is purposefully broad and accounts for each layer of cyberspace (physical, logical, and cyber-persona). Understanding the interplay between the three layers is crucial for understanding cyberspace. The physical layer is "comprised of the geographic component and the physical network component." Included are organic servers located in sovereign nations and the associated physical equipment connecting servers to other points globally. The logical layer refers to locations that exist in cyberspace. "A simple example is any Web site that is hosted on servers in multiple physical locations where all content can be accessed through a single uniform resource locator." The cyber-persona refers to the digital representation of an actual person interacting within the logical layer. Examples include email and IP addresses, cell phone numbers, and social media (Twitter, Facebook, etc.). However, "A single cyber-persona can have multiple users. Consequently, attributing responsibility and targeting in cyberspace is difficult." Additionally, a cyber-persona can be created with the intent of

[20] Joint Chiefs of Staff (JCS), Joint Publication (JP) 3-12 (R), *Cyberspace Operations* (Washington, DC: Government Printing Office, 5 February 2013), GL-4.

concealing the individual's actual identity. The DoD definition of cyberspace appreciates the interplay across each layer of cyberspace.[21]

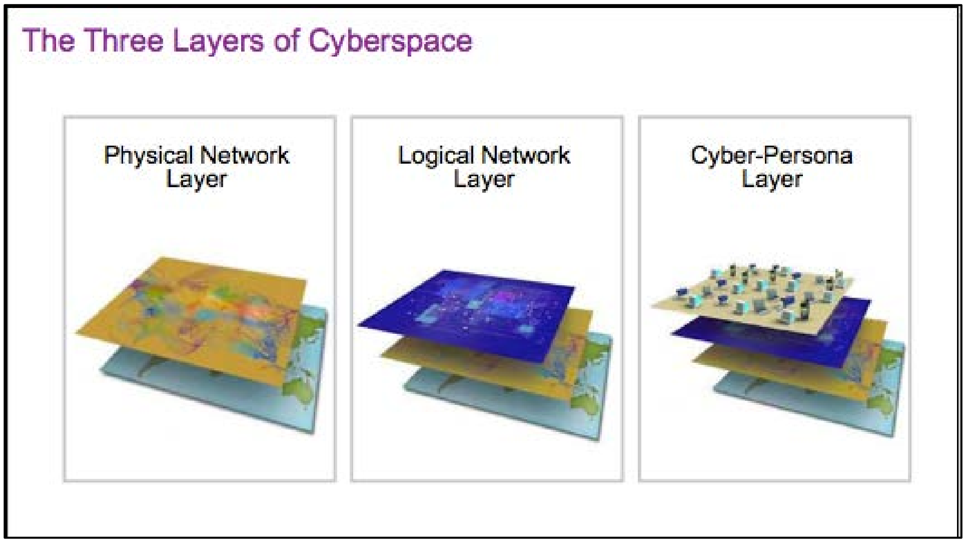

Figure 1. The Three Layers of Cyberspace

Source: Joint Chiefs of Staff, Joint Publication 3-12 (R), *Cyberspace Operations* (Washington, DC: Government Printing Office, 5 February 2013), I-3.

The combination of physical and logical layers creates a network. "Networks are systems that are formed by links . . . Networks share information and use various methods to direct the manner in which information flows." Networks come in varying sizes depending on their characteristics and function. For example, a personal-area network "is a network that connects devices, such as mice, keyboards, printers . . . within range of an individual person." A local-area network connects people "within a common

[21] JCS, JP 3-12 (R), v – 1-4.

organizational structure." Ever larger is the wide-area network, which "connects multiple smaller networks such as local-area networks that are in geographically separated locations." The Internet is a wide-area network built on an ever-expanding network of globally dispersed wide-area networks. The interconnected nature of the Internet allows people to transmit information at the speed of light. This is possible because information is "broken" into "packets," sent the quickest way possible and reassembled at the destination. Essentially the data follows the path of least resistance. This means data may travel through servers located in other countries. This process is possible for two reasons. First, the Internet was built on the rapid, open, and free flow of information. Second, every "node" in the network has an "address" making it possible to deliver data to the precise location. The physical infrastructure creates the logical layer of cyberspace, which in turn creates an environment conducive to the development of cyber-personas.[22]

Peter Singer and Allan Freidman, in *Cybersecurity and Cyberwar: What Everyone Needs to Know* (2014), provide an excellent overview of the cyber domain and addresses nearly every topic in the current literature related to cybersecurity. Peter Singer is a Senior Fellow at the New America Foundation and considered a preeminent futurist. Allan Friedman, a Brookings Institute Fellow, is a distinguished cybersecurity professional with expertise in public policy and computer science. As noted in the title, this book was written for an educated general audience that may not have a technical background. The book is divided into three parts. Part one answers the question, "How does the Internet work?" This section grapples with the concept of "security" and

[22] Cisco Networking Academy, *IT Essentials: PC Hardware and Software Companion Guide,* 5th ed. (Indianapolis, IN: Cisco Press, 2014), 299-304.

discusses the Central Intelligence Agency-developed security triad comprised of confidentiality, integrity, and availability. “Confidentiality refers to keeping data private . . . Integrity means that the system and the data in it have not been improperly altered or changed without authorization . . . Availability means being able to use the system as anticipated.” The “CIA triad” identifies the aspects of security that are most important to the proper functioning of cyberspace and consequentially a target for exploitation.

One side of the security coin is trust. Trust in the network encourages users to cooperate in the cyber domain and intrinsically emboldens people to participate in social media, to buy and sell online, and to store vast amounts of sensitive data in “clouds.” However, repeated violations of this trust and a perceived lack of security “undermine(s) trust in the broad digital systems.” In this sense, trust constitutes cyber’s source of power. The other side of the security coin is network resiliency. As the authors note, “Resilience is what allows systems to endure security threats instead of critically failing.” Resiliency is about “understanding how the different pieces fit together and then how they can be kept together or brought back together when under attack.” Simply put, network resiliency allows public and private industries to maintain connectivity and reduce service interruptions.[23]

Part two of Singer’s and Friedman’s book looks at how cyber attacks target vulnerabilities. The section provides an excellent overview of the most salient attacks and how they were employed. A key concept addressed is attribution, which refers to the

[23] Peter W. Singer and Allan Friedman, *Cyberspace and Cyberwar: What Everyone Needs to Know* (New York: Oxford University Press, 2014), 35-36, 173.

ability to accurately identify an attack's architect and executer. "It is sometimes possible to track an actor's efforts to a certain geographic locale, but it is more difficult to establish any formal government role." Arguably, high confidence attribution constitutes a barrier to the creation of coherent and enforceable cyber laws. The authors also discuss the difficulties defining cyberwarfare arguing that, "We are still at the early stages of conceptualizing what cyberwar will look like." This reasoning concedes that the term cyberwar, although rampant throughout the literature, remains elusive. One reason for the ambiguity is that, to date, no fatality can be directly attributed to a cyber attack, effectively falling short of the U.S. requirement that an act of war needs to "proximately result in death, injury or significant destruction." Instead, we are left living in perpetual state of cyber conflict. This section also discusses the offense-defense balance stating that, "the cyber competition will be offense-dominant for the foreseeable future," however, the ability to correctly anticipate the second and third order impacts of an offensive cyber attack may reduce actual offensive effectiveness. The authors argue that, "The most important lesson we have learned in traditional offense-defense balances, and now in cybersecurity, is that the best defense actually is a good defense." Meaning, that improving cybersecurity through improved defensive capabilities and network resiliency can impose higher costs on the offense, creating "deterrence by denial."[24]

In order to appreciate the relevance and scope of a cyber attack it is necessary to briefly review a few of the best-documented occurrences. Two of these attacks (Stuxnet and Chinese-sponsored cyber espionage) are analyzed in the individual case studies. In

[24] Singer and Friedman, 74-155.

April 2007, Russian hackers conducted a series of cyber attacks against Estonia. This event marked another important evolution in the conceptual development of cyber as a weapon. In this case Russian "patriotic hackers" launched a series of distributed denial of service (DDoS) attacks against the government of Estonia. Patriotic hackers are individuals that self-organize into amorphous groups to, "Carry out cyberattacks on perceived enemies of that state, without explicit, official state encouragement or support."[25] The effects stunned the government of Estonia. "Suddenly Estonian banks, media web pages, and government websites were hit with a large-scale denial of service attack." However, it should also be noted that the series of DDoS attacks "had little impact on the daily life of the average Estonian and certainly no long-term effect." Nonetheless, it did lead to the establishment of the NATO Cooperative Cyber Defense Centre of Excellence and the "Tallinn Manual on the International Law Applicable to Cyber Warfare."[26]

Russia's cyber attacks against Estonia were instructive for three reasons. One, the Estonia Government attempted to initiate the North Atlantic Treaty's Article Five, however, member states, including the United States, determined that the attacks did not meet the threshold for mobilizing North Atlantic Treaty Organization military forces. Second, the attacks demonstrated the impact a group of resourceful and cyber savvy

[25] Singer and Friedman, 298.

[26] Ibid., 99-123.

individuals could have against a sovereign government. Third, the North Atlantic Treaty Organization instituted Estonia as the cybersecurity executive agent for the alliance.[27]

In 2010, cybersecurity professionals became aware of a particularly complex piece of malware that infected thousands of computers worldwide. The malware was spillage linked to Stuxnet. Stuxnet was a powerful piece of malware designed to deliberately destroy Iranian nuclear centrifuges. Stuxnet's exact origin is unofficially attributed to the United States and Israel. Stuxnet was constructed to conduct several missions simultaneously. The more destructive aspect adjusted the pressure within nuclear centrifuges and manipulated the speed of the spinning rotors. It accomplished this while ensuring the instrument readings remained within normal operating parameters, effectively "tricking" Iranian nuclear experts to trust their system. Stuxnet carried out its operations undetected for over a year and rolled Iranian nuclear ambitions back approximately five years. There are three things particularly unique about Stuxnet. One, the malware was extremely complicated and incorporated multiple zero day attacks. A zero day refers to, "An attack that exploits a previously unknown vulnerability." Second, it attacked an air-gapped system meaning that the targeted system was physically isolated from any logical network. Third, it demonstrated that a cyber attack could destroy critical infrastructure in the physical world.[28]

China's ongoing cyber espionage operations demonstrate another foundational cyber capability. These operations are classified as advanced persistent threats (APT),

[27] Robert Kaiser, "The Birth of Cyberwar," *Political Geography* 46 (2015): 19.

[28] Kaiser, 115-118.

which are, “Cyberattack campaign[s] with specific, targeted objectives, conducted by a coordinated team of specialized experts, combining organization, intelligence, complexity and patience.”[29] APTs, and specifically the Chinese variant, are difficult to detect, isolate, and eradicate. Countering Chinese cyber espionage requires immense resources in terms of money, personnel talent, and time. All of which, depending on the fiscal situation, may be limited. “The data [the Chinese] made off with included national security secrets, product design schematics, and negotiation plans.” The information stolen is not just of political or military relevance, but economic, leading to a “historically unprecedented transfer of wealth.”[30]

China’s ceaseless cyber espionage indicates three trends. First, the rampant intrusions emphasize the importance of properly protecting the vast amounts of IP contained in cyberspace. A failure to safeguard this information impacts the nation’s economic health. Second, the attacks demonstrate that a successful cyber espionage campaign can extract an incredible amount of data without needing to physically violate a nation’s borders. Third, the severity indicates that these types of persistent threats will continue unabated until sufficiently affordable and realistic counter-measures are created and implemented.

An analogy in the physical domain would be multiple small units clandestinely infiltrating a city via overland routes in order to conduct special reconnaissance activities that enabled operators to extract multitudes of IP and personal information either

[29] Singer and Friedman, 293.

[30] Ibid., 92-95.

instantly or over a longer duration. Another example would be a strategic bomber capable of destroying an industrial complex without killing a single person. These imperfect examples are simply aids to visualize how activities in the cyber domain are not confined to one type of mission or technique. It also shows that in certain ways cyber attacks, with the capacity to conduct operations absent an actual physical penetration, are more exploitative than conventional attacks. Additionally, it is assumed that a nation with the technological potential would want to have both capabilities, making the development of effective defensive measures a matter of national security.

Part three of Singer's and Friedman's *Cybersecurity and Cyberwarfare* provides recommendations for safeguarding the cyber domain. The authors identify three elements that will create a more resilient system. "One is the importance of building in 'the intentional capacity to work under degraded conditions.' Beyond that, resilient systems must also recover quickly, and finally learn lessons to deal better with future threats."[31]

The authors argue in favor of building "a network of treaties and norms." This would include creating organizations authorized to establish and enforce standards of conduct in the cyber domain. Internationally this would require developing mutually accepted guidelines similar to those under the law of armed conflict. However, problems associated with high confidence attribution and the advanced cyber capacities of large developed countries continue to inhibit the creation of such laws.[32]

[31] Singer and Friedman, 171.

[32] Ibid., 179-186.

The third strategy includes increasing baseline knowledge of current cyber issues and opportunities throughout "the public and private sectors." Arguably, Singer and Friedman had this in mind when they wrote their book. Much of cyber's fundamentals remain out of reach for most people due to a combination of a lack of technical knowledge, no experience with cyber attacks, and a general lack of interest.[33]

Finally, the authors identify five trends that continue to shape the cyber domain which are: "the rise of cloud computing, big data, the mobile revolution, a demographic shift in the makeup of those who consider cyberspace home, and the internet of things." In cloud computing, "individual machines become less important, and instead the companies that control the data and access to it play an increasingly essential role." The rise and importance of big data may lead to the breakdown of "human social, legal, and ethical boundaries we aren't yet ready to cross."[34]

The mobile revolution resulted in the development of "smart" phones enabling portable access the Internet. However, this connectivity provides a vulnerability that can be attacked. "Mobile devices have smaller interfaces that offer less security information, and have fewer computational resources for defense."[35] Arguably, the mobile revolution not only demonstrates the day-to-day relevance of cyber but also reveals cyber's trajectory. Technological advancements increasing capacity at the logical layer enable the deeper development and refinement of individual cyber-personas. For example, a few

[33] Ibid., 197.

[34] Ibid., 248-253.

[35] Ibid., 251.

decades ago it was inconceivable to assume that mobile phones would replace landlines or that people would rely on smart phones to socialize and conduct business. The mobile revolution promotes greater access to the logical layer not for connectivity's sake but as a way to generate greater development and utilization of each person's cyber-persona. We are witnessing a situation where our cyber-personas are becoming inextricably linked to our actual selves. This represents a key aspect of the cyber domain that cyber experts are only beginning to fully appreciate.

Additionally, a demographic shift is altering the geographic, cultural, and linguistic origin of the preponderance of cyber-personas in cyberspace. For example, the United Nations "predicts that Chinese-speaking users of the Internet will outnumber English speakers by 2015." Finally, the Internet of Things, which refers to the plethora of household appliances and other devices connecting to the Internet, promises to be the next frontier in efficiency. However, it "also enables cyberattacks to penetrate far deeper into our lives than ever before." The five trends identified constitute key variables that can alter the application of national power in cyberspace.[36]

In conclusion, the complex interplay among the three layers of cyberspace (physical, logical, and cyber-persona) creates a unique environment producing unprecedented opportunities and challenges. For example, a technological breakthrough

[36] Singer and Friedman, 252-254. As of early 2016, it is reported that over half of China's population (over 7 million, people or 52.2%) are connected to the Internet; Melanie Lee, "China's Nearly 700 Million Internet Users Are Hot for Online Finance," *Forbes*, 25 January 2016, accessed 7 May 2016, http://www.forbes.com/sites /melanieleest/2016/01/25/chinas-nearly-700-million-internet-users-are-hot-for-online-finance/#5418bad81391; Internet Live Stats, "China Internet Users," accessed 7 May 2016, http://www.internetlivestats.com/internet-users/china/.

or efficiency gained in one layer translates into a new utility or application in another layer. Additionally, a vulnerability exploited in one layer can reverberate across the other levels, specifically cyber-persona, and oftentimes in ways that are unforeseen. It is also true that while our reliance on cyberspace enabled interaction continues to increase cyber experts and policy makers are only beginning to grapple with the second and third order effects. The next section looks at how the cyber literature perceives the opportunities and challenges present in cyberspace.

Cyberwar Literature

A baseline understanding of cyberspace is important before discussing the cyber literature; otherwise it is difficult to determine an argument's strengths and weaknesses. An excellent starting point is Chris Demchak's and Peter Dombrowksi's, "Rise of a Cybered Westphalian Age," which argues that Stuxnet ushered in a "cybered Westphalian age" characterized by "virtual borders and national cyber commands as normal elements of modern cybered governments." Demchak and Dombrowksi maintain that cyberspace created frontiers that rapidly transformed into commons. These under-governed spaces are hotbeds for conflict due to an absence of mutually understood rules or entities capable of enforcing standards. This vacuum creates issues for states in terms of sovereignty and the legitimate use of force. "Being able to establish sovereign control is a hallmark of a functioning state." As noted, cyberspace includes physical infrastructure engineered to create the logical layer. Real people are then able to develop a cyber-persona and interact within the logical layer. A "cybered Westphalia" refers to a state's difficulty exerting control over the logical layer, which translates into a reduced ability to protect physical infrastructure and citizens' cyber-personas. "The cybersphere has challenged the security of individuals and states themselves in ordinary systems considered essential to the critical functions of society."[37]

Demchak and Dombrowski argue in favor of creating cyber borders. "A cybered national border is technologically possible, psychologically comfortable, and systemically and politically manageable." China's "Great Fire Wall" regulates traffic through one of its three "Internet gateways" and the "Golden Shield" allowing a cyber police force to troll the web for nefarious activity (e.g. political dissidents). The U.S. approach created a military cyber command with the mission to attack and defend in cyberspace. The authors argue that the state "is explicitly saying it has territory to defend and the threat to be met poses conceivably an existential threat." The article does an excellent job explaining how the growth of cyberspace and the lack of governing laws undermine state sovereignty.[38]

A criticism of the article is that Demchak and Dembrowski overlook the currently unresolved problem of attribution. It is understood that states want to control their territory and protect their population, but attribution makes it difficult to develop coherent laws that receive international recognition. Also not covered is the idea that large technologically advanced states may actually benefit from the lack of international rules. Additionally, the article glosses over fact that the Treaty of Westphalia was made possible after thirty years of war and violence consumed Europe. A key question is, does it follow that conflict (cyber or physical) will precede the creation of any accepted cyber

[37] Chris C. Demchak and Peter Dombrowski, "Rise of a Cybered Westphalian Age," *Strategic Studies Quarterly* (Spring 2011): 32-61.

[38] Ibid., 39-50.

boundaries or laws? In other words, are high levels of conflict necessary before the issue receives the attention of global decision makers?

The literature also discusses the possibility of a cyber attack with the destructive equivalence of the attack on Pearl Harbor or nuclear explosion. In 2012, Secretary of Defense Leon Panetta warned that a potential cyber-Pearl Harbor launched against the United States remained a real concern.[39] He noted that a "cyber-Pearl Harbor . . . would cause physical destruction and the loss of life, an attack that would paralyze and shock the nation and create a profound new sense of vulnerability." Arguably, Panetta was speaking openly about the threat in order to build public awareness and encourage congress to pass legislation authorizing funds dedicated to improving the United States' cyber capabilities. Panetta argued that, "If we detect an imminent threat of attack that will cause significant physical destruction in the United States or kill American citizens, we need to have the option to take action against those who would attack us, to defend this nation."[40] Panetta's stark warning is a reminder that perceived US cyber dominance is expected but not guaranteed and that unseen cyber jockeying amongst nations continues at full speed.

Quan Hai T. Lu, a U.S. Army major at the Defense Threat Reduction Agency, argues in, "Cyber Attacks: The New WMD Challenge to the Interagency," that "cyber is the new weapon of mass destruction threat, and addressing it will require marshaling the

[39] Elisabeth Bumiller and Thom Shanker, "Panetta Warns of Dire Threat of Cyberattack on U.S.," *New York Times*, 11 October 2012, accessed 9 December 2015, http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?_r=0

[40] Ibid.

resources of the entire interagency." Lu points to the advent of the Internet of Things and a deeply entrenched reliance on cyber managed critical infrastructure as a reason cyber attacks can achieve weapons of mass destruction results. These systems are commonly referred to as Supervisory Control and Data Acquisition (SCADA). SCADA is defined as, "A type of industrial control system, particularly used to monitor and manage interconnected sensors and control large facilities."[41] SCADA systems are frequently associated with critical infrastructure. Lu argues that, "The electric grid is the US technological center of gravity" and "the vulnerability of the electric grid industrial control systems to cyber attacks and other critical infrastructure has given adversaries of the United States a relatively easy way to disrupt or destroy US civil society." Lu identifies other U.S. industries such as the health care system, nuclear reactors, and water treatment facilities as equally appealing targets. The author notes that it is almost a mystery that the United States has not suffered such a disaster and identifies three possible explanations. One, actors may lack the capabilities to successfully launch an attack. Second, those with the capacity may fear a U.S. response. Third, adversaries may be more interested in stealing industrial knowledge. These explanations may demonstrate the efficacy of deterrence. Lu concludes that the DoD and Department of Homeland Security should combine their collective resources to develop effective strategies to deter a potentially successful cyber attack against U.S. critical infrastructure.[42]

[41] Singer and Freidman, 298.

[42] Quan Hai T. Lu, "Cyber Attacks: The New WMD Challenge to the Interagency," *Interagency Journal* 6, no. 2 (Spring 2015): 48-57.

James J. Wirtz, associate professor of National Security Affairs at the Naval Postgraduate School, argues that, "The United States is vulnerable to a 'Cyber Pearl Harbor' and it is possible to anticipate how and why it will occur." Wirtz suggests that the United States is actually "more likely to be the victim, not the initiator, of a Cyber Pearl Harbor." He argues that U.S military superiority and immense assortment of SCADA controlled infrastructure may convince a technologically advanced but militarily weaker adversary to launch a preemptive attack aimed at neutralizing the United States. If such an attack did occur Wirtz notes, "the degradation of US military capabilities caused by a cyber attack will eventually be overcome, but the political and strategic consequences of a failure of deterrence will linger long after US forces recover their full capabilities." Most disturbing is the prospect that U.S. military leaders underestimate this threat. A cyber attack on the magnitude of Pearl Harbor would result from a caustic cocktail of intelligence failures, technological surprise and a failure of deterrence. "The effects of the Cyber Pearl Harbor . . . will have a lasting political and strategic impact on US interests." The solution, according to Wirtz, is to develop sufficient cyber capabilities that emphasize "deterrence by denial," designed to convince an adversary that "there is little opportunity to achieve asymmetric effects by employing cyber attacks." [43]

A cyber attack analogous to Pearl Harbor or a nuclear strike rests on the supposition that offense holds the advantage and that vulnerable nations simultaneously

[43] James J. Wirtz, "The Cyber Pearl Harbor," in *Cyber Analogies,* ed. Emily O. Goldman and John Arquilla (Technical Report, Naval Postgraduate School, Monterey, CA, 28 February 2014), 7-14.

suffer from an over reliance on cyberspace for the management of critical systems. Therefore they fail to deter adversaries successfully or defend vulnerable systems.

Cyber literature discusses the offense-defense balance from a variety of perspectives. Keir Liber, a faculty member at the Center for Security Studies at Georgetown University, observes that according to offense-defense theory if technological innovations increase mobility then offense is favored, while innovations increasing firepower favor defense. This distinction is important for understanding what role cyber might play in interstate conflict and the cyber attacks most likely to achieve their objectives. The author concedes that applying offense-defense theory to cyber is difficult but nonetheless argues that, “Both existing and new criteria point to a clear offensive advantage in cyberspace.” An offensive advantage may mean that cyber attacks are likely to increase until sufficient defensive measures are created. “Based on the ODT literature, it seems reasonable to worry that the current era of cyber offensive advantage could spell trouble.” However, the capacity to conduct an offensive cyber attack does not automatically guarantee an attacker can achieve their end state. “The most general reason to doubt the utility of the offense-defense balance analogy in cyberspace stems from enormous uncertainty about whether cyber attacks can inflict significant military damage on a victim.” Furthermore, it remains undetermined if cyber attacks, regardless of severity, can lead to a political victory. For this reason Liber concludes that a “cyber

Pearl Harbor" is not realistic and despite cyber's current offensive advantage it is unlikely to convince weaker states to strike a strong state.[44]

Patrick J. Malone, in his 2012 Naval Postgraduate School master's thesis, provides clarity to the offense-defense balance discussion by focusing on the amount of money spent on either cyber offense or defense. His heuristic based model analyzed Russia's cyber attack against Estonia in 2007 and Stuxnet. In the case of Estonia the offense-defense ratio was 1:424, meaning that for every $1 spent on offense the defense spent $424, while the ratio for Stuxnet was slightly better at 1:7. Overall, Malone calculated the offense-defense balance ratio to be 1:132. While the author concedes that the model is imperfect it is a startling indicator of the efficacy of cyber offensive action. However, the thesis does not discuss the cost of more traditional forms of defense like routine law enforcement or conventional military capabilities. Arguably, the cost of defense is usually higher than offense. However, this does not detract from Malone's conclusion because by highlighting the disparity he emphasizes, that similar to conventional weapons, large and wealthy states are the most likely to be able to afford defensive measures, while smaller poorer nations may lack the ability to wage effective cyber offense or defense.[45]

RAND researcher, Martin C. Libicki, is an expert on cyber conflict. In his book *Conquest in Cyberspace: National Security and Information Warfare* (2007), he posits

[44] Kier Lieber, "The Offense-Defense Balance and Cyber Warfare," in *Cyber Analogies*, ed. Emily O. Goldman and John Arquilla (Technical Report, Naval Postgraduate School, Monterey, CA, 28 February 2014), 96-107.

[45] Patrick J. Malone, "Offense Defense Balance in Cyberspace: A Proposed Model" (Thesis, Naval Postgraduate School, Monterey, CA, December 2012), 1-66.

that even the most devastating information warfare scenario, which in this context is understood to be cyber attacks, is more comparable to a snowstorm than a nuclear explosion. Libicki argues that the effects of a cyber attack itself "is entirely temporary and rapidly over." For example he concludes that, "Nuclear war creates firestorms, destroying people and things for miles around. By contrast, even a successful widespread information attack has more the character of a snowstorm . . . But the effects of snowstorms, apart from a few random heart attack and accident victims, is entirely temporary and rapidly over." However, what if the snowstorm was manmade by an adversary? Would that change people's perception of a proportional response? Would that affect their patience with the restoration of services? Would people quickly grow tired of throwing snowballs and opt for a firestorm? Libicki's fire versus snowstorm analogy provides a compelling argument but it fails to address people's natural response to being threatened and attacked.

Furthermore, Libicki argues that the hostile conquest of cyberspace may be less than can be accomplished through friendly conquest. Friendly conquest actualizes Joseph Nye's smart power theory and argues that technologically advanced nations, such as the United States, can create an asymmetric dependence. Asymmetric dependence refers to a state's ability to create an "information system attractive enough to entice other individuals or institutions to interact with it by for instance, exchanging information or being granted access." Friendly conquest still denotes conquest and a possibility for miscalculation and the initiation of a security dilemma centered on owning elements of cyberspace.[46] It is clear that Libicki is wary of any national policy or strategy that overstates cyber's capacity to achieve a defined end state through offensive action. When asked if cyberspace matters, he responds that "the best answer . . . is neither 'yes' or 'no' but 'more so everyday'."[47]

Andrea Little Limbago, a principal social scientist at a security intelligence and analytics company, argues that instead of focusing on the offense-defense balance policy makers could do better by recognizing the existence of a "cyber statecraft spectrum." One side of the spectrum includes "soft power" cyber options while the other contains "hard power" capabilities. For example, a soft power option would be investment in Internet infrastructure and access; while hard power would be offensive cyber attacks. In between are factual information and data dissemination, propaganda, and censorship. Little Limbago observes that, "cyber statecraft is unique in its asymmetric nature, capable of empowering not only major powers but also serving as a means for weaker actors to have a disproportionate impact in the international arena." In other words, the state does not own a monopoly on the use of cyber as a form of statecraft. Additionally a myopic focus on cyber's offensive proclivities inhibits the development of creative soft power applications. Little Limbago argues that the "focus on cyber's offensive manifestations

[46] See Kevin Pollpeter's, "Chinese Writings on Cyberwarfare and Coercion," in *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, ed. Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (New York: Oxford University Press, 2015), 138-162. Pollpeter argues that China views the current U.S. dominance of the Internet as a critical vulnerability for China that can only be countered by creating a strong indigenous competitor in terms of physical and logical layer infrastructure.

[47] Libicki, *Conquest in Cyberspace*, 3-291.

ignores the nuanced nature of this critical domain and its broader application to geopolitics."[48]

John Kao, a former professor at Harvard's School of Business and self-described "innovation activist," describes the characteristics that enable Silicon Valley to maintain its status as a nucleus of innovation and how embracing aspects of this culture can help cybersecurity professionals solve their most pressing problems. Kao notes that, "the Silicon Valley dynamic is not typically a linear progression from idea to funding to execution, but rather the expression of a web or relationships, an ecosystem in which there are many pathways to yes." The emphasis on nonlinear funding and the importance of diverse relationships allows the full expression of ideas and solutions to develop. This is important in an industry like cybersecurity, which relies on developing innovative solutions faster than an adversary can exploit a vulnerability or conduct a crippling cyber attack. However, Kao notes that Silicon Valley is quickly losing its status as the premiere innovation center and that "it is clear that there are at least 50 countries around the world with sophisticated national innovation agendas, strategies, and investment programs." What this means is that as more countries seek to close the innovation gap they will simultaneously rely less on U.S. developed technology making the United States less competitive in the international market. One of these countries is China who invested "$500 billion into its national innovation agenda." This poses a direct threat to the U.S. cybersecurity industry in that other countries may be able ellipse U.S. prominence thus creating inherent vulnerabilities and forcing the United States to play catch-up. To avoid

[48] Andrea Little Limbago, "One Size Does Not Fit All: The Multifaceted Nature of Cyber Statecraft," *Joint Force Quarterly*, no. 78 (3rd Quarter 2015): 84-90.

this undesirable situation Kao recommends that, “The cybersecurity community will have to learn how to build relationships across the hard skin of organizational boundaries, to be able to establish friendships, alliances, partnerships and collaborations that don’t fit the traditional model of defense contracting.”[49]

Political scientist, Erik Gartzke, argues that advocates of cyberwarfare have “yet to work out how cyberwar enables aggressors to accomplish tasks typically associated with terrestrial military violence.” Furthermore, “the chief beneficiaries of cyberwar . . . [are] more likely to be nation-states.” This contention flies in the face of arguments pointing out cyber’s asymmetric essence and capacity to achieve devastating effects. Upon closer inspection of Stuxnet and Russia’s cyber attacks against Georgia the data seems to indicate that even if non-state actors can obtain cyber capabilities the real expertise and relevance will belong to large nation-states. In fact, Gartzke argues that, “cyberwar should be particularly appealing to capable states confronting weaker opponents . . . cyberwar may perpetuate or even increase military inequality.” Gartzke concludes that, “Cyberwarfare will most often occur as an adjunct to conventional warfare, or as a stop-gap and largely symbolic effort to express dissatisfaction with a foreign opponent.” In other words, cyberwar is a misnomer. The correct term should be cyber attack or cyber conflict, which recognizes that employed detached from a broader conventional approach cyber is unlikely to achieve the anticipated end state.[50]

[49] John Kao, “Silicon Valley: Metaphor for Cybersecurity, Key to Understanding Innovation War,” in *Cyber Analogies*, ed. Emily O. Goldman and John Arquilla (Technical Report, Naval Postgraduate School, Monterey, CA, 28 February 2014), 90-95.

[50] Erik Gartzke, “The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth,” *International Security* 38, no. 2 (Fall 2013): 41-73.

Conclusion

The current literature analyzes cyberwar from a variety of perspectives. While identifying the most salient digital weapon remains debatable, it is clear that comprehending and uncovering cyber's efficacy remains an important endeavor. Cyber as a domain continues to evolve in unanticipated ways and with implications that are ambiguous at best.

Cyber laws and the creation of cyber boundaries continue to be a topic of discussion, but have not materialized. There are several reasons for this, not least of all is the issue with attribution and the opinion that nations (specifically those with strong cyber capabilities) benefit from an anarchic system. Does this equate to a "cybered Westphalia?" If the answer is yes, does that mean society is we on the cusp of an open ended and dynamic cyber conflict? How does the ever-increasing importance of the our cyber-persona necessitate the establishment of cyber laws and boundaries? These questions continue to be debated.

Perhaps the most compelling arguments analyze cyber's offense-defense balance. According to many researchers, the assessment that the cyber domain permits greater mobility indicates that offense holds the advantage. However, this does not denote an outbreak of "total" cyber conflict, but will increase the frequency of cyber attacks. It also places an impetus on building robust defense capabilities. One researcher concludes that the offense-defense cost ratio is 1:132 in favor of offense. This means that it is probable that only wealthy and technologically advanced countries will be able to afford strong defensive capabilities. This leaves poorer countries more vulnerable.

It seems clear that researchers and policy makers alike are scrambling to stay ahead of the technology and its potential utility as a weapon. This sense of urgency is warranted. As Silicon Valley and other innovation centers around the world continue to make technological breakthroughs, policy makers and defense officials are left contemplating, “So What?” At some point a peer competitor may ellipse the United States in terms of technological innovation and subsequent technology export. Undoubtedly, this situation places the United States at a disadvantage in terms of safeguarding network systems and alters the concept of the “friendly conquest of cyberspace.”

Additionally there is a vigorous debate over the meaning of cyberwar and its existence. Can a cyber campaign divorced from conventional action achieve political objectives? To date, this has not occurred. However, it is does not mean it is impossible. It does mean that incentives exist for correctly calculating cyber’s potential and calibrating apportionment towards construction of a range of cyber capabilities. The nation with the means and foresight will create a robust cyber capability for two reasons. First, to conduct offensive cyber operations, including cyber industrial espionage and attack critical infrastructure. Second, to deter adversaries. In this sense, it is not just about ensuring vital systems are impenetrable, or at least resilient, but also about deterrence by denial.

Cyber experts continue to debate the likelihood of a cyber attack equivalent to Pearl Harbor or a nuclear strike. Researchers supporting this view cite the expanded reliance on SCADA controlled critical infrastructure, which despite being air gapped, remain susceptible to a sophisticated attack. Detractors argue that the threat of such an attack is overblown and unrealistic. This may be true. However, researchers should assess the impact of a "Cyber Desert One," meaning a U.S. sponsored cyber attack that fails spectacularly on the world stage.[51] Such a crisis may critically damage U.S. credibility and paralyze decision makers. This could result from inadequate funding, a vague chain of command, and lack of validated interagency interoperability. Arguably, the United States has made great strides towards overcoming such a situation through the establishment of U.S. Cyber Command and the strong operational links to the National Security Agency. However, it is entirely possible that due to cyber's "newness" and high classification requirements that stove piping and a lack of authorities could inhibit success at a critical moment.

[51] Officially called Operation Eagle Claw, Desert One refers the 1980 failed hostage rescue of U.S. Embassy personnel held in Tehran. The U.S. population was well aware of the situation and in the months leading up to the operation received nightly updates. Arguably, this awareness and subsequent national angst made freeing the hostages a moral issue for the Carter Administration. Consequently, the botched operation was an embarrassment for Carter and the United States in general. As a result, no further rescue attempts were authorized. Ironically, the tragedy was a catalyst for change and resulted in greater funding and support for special operations and the creation of the Joint Special Operations Command.

CHAPTER 3

LH AND THE INDIRECT APPROACH

LH Background

Basil Henry Liddell Hart, an Englishman, was born in Paris, France, in 1895. His preoccupation with military affairs manifested itself early in his childhood and was marked by a “precocious tactical interest in boyhood games.” Although decidedly non-athletic, LH participated in multiple sports and remained a voracious reader of military history throughout his youth. In 1913, he attended Corpus Christi College, Cambridge, to study modern history. In 1914, “shortly after the outbreak of the First World War Basil Hart was among the thousands of young men who answered Kitchener’s call for volunteers.” As a British soldier, he was sent to the Western Front on two occasions. His second trip was in spring of 1916, where he served in the tactical reserve for the initial action of the Somme offensive. “His battalion . . . was practically wiped out on the first day, which cost the Army nearly 60,000 casualties – the heaviest day’s loss in British history.” LH’s experiences in WWI heavily influenced the subsequent development of his military theories.[52]

Immediately following WWI, while still on active duty, LH wrote extensively on infantry tactics and in June 1920 published his famous essay, “Man in the Dark.”[53] LH developed the “Man in the Dark Formula” as a visualization tool to describe combined

[52] Bond, 12-17.

[53] John J. Mearsheimer, *Liddell Hart and the Weight of History* (Ithaca, NY: Cornell University Press, 1988), 26.

arms maneuver built around mobile platoon sized elements. The evolution of LH's method contrasted sharply with the French military establishment's preoccupation with division sized "methodical battles." LH's intent was to develop an approach that avoided the "bloody frontal assaults of World War I" and instead maximized speed and economy of force to achieve overall success through the efforts of "thousands of platoon sized successes."[54] Throughout the 1920's LH continued to develop and refine his "formula" and wrote multiple essays and articles promoting the method and praising the decision making of the British General Staff throughout the war. Consequently, prominent British leaders, such as General Sir Ivor Maxse, took notice of LH's ideas and saw value in his tactical recommendations.[55] In the years leading up to 1924, LH continued to write extensively on the efficacy of infiltration tactics and mechanized warfare. Many of his concepts reached the ears of British generals. However, in 1924, due to recurrent medical conditions LH was discharged from the Army effectively ending any aspirations of "remaining a professional soldier."[56] With the assistance of General Sir Ivor Maxse, he was given a job as journalist at the *Morning Post*. Soon thereafter he became the military correspondent of *The Daily Telegraph*, a position he held for ten years.[57]

[54] Mearsheimer, 27.

[55] Bond, 19. General Maxse served as the British Army's Inspector General of Training.

[56] Ibid., 32.

[57] Ibid., 33.

Towards the end of 1924, LH moved beyond the study of tactics and into the realm of the operational and strategic levels of war.[58] As the 1920s progressed LH furthered developed his understanding of the events of WWI. Through his study he became increasingly disillusioned with the skill of British generalship during the war. It is from this perspective that he sought to develop a "general theory of strategy."[59] In 1929 he published, *The Decisive Wars of History*. In many ways this book represents the amalgamation of his tactical recommendations as articulated in his "Man in the Dark Formula" with his development of the indirect approach at the strategic level. His central conclusion was that, "The soundest strategy in any campaign is to postpone battle, and the soundest tactics to postpone attack, until the moral dislocation of the enemy renders the delivery of a decisive blow practicable."[60] The emphasis on the moral dislocation prior to an attack comprises the essence of LH's indirect approach and while he continued to adapt the means he consistently believed in the efficacy of an indirect approach. In 1954, LH conducted a major update and retitled the book, *The Strategy of the Indirect Approach*. In 1967, he again published an updated edition, which included effusive praise from former German and Israeli military commanders extolling LH's influence on their understanding and employment of the indirect approach in general and blitzkrieg in particular.[61] In 1970 LH passed away.

[58] Ibid.

[59] Bond, 34.

[60] B. H. Liddell Hart, *The Decisive Wars of History: A Study in Strategy* (London: Bell, 1929), 146.

[61] Mearsheimer, 1.

Throughout the interwar years LH's reputation as a sage military theorist achieved its zenith. British military officers and political leaders consumed his theories and entertained his recommendations. However, at the outbreak of WWII, and in the years immediately thereafter, British Government leaders and several academics branded LH a snake oil salesman and accused him of selling the British people a flawed strategy.[62] He invested his remaining years to rebuilding his reputation.[63] The remainder of this section will look at how LH's theories developed over time and how he was able to rescue his reputation from the dustbin of history.

LH: Armored Warfare vs. The Indirect Approach

There are two principal books analyzing the development of LH's military theories. One is Brian Bond's, *Liddell Hart: A Study of His Military Thought* (1976), and the second is John J. Mearsheimer's, *Liddell Hart and the Weight of History* (1988). Brian Bond knew LH personally and worked with him on several projects. John J. Mearsheimer's book, published twelve years after Bond's, was largely in reaction to Brian Bond's and sought to apply a deeper level of critical analysis.

Brian Bond was a student at Oxford when he first met LH in 1959. LH mentored Bond and helped him launch his career as a military historian. Bond and LH had initiated work on a military history project when LH unexpectedly passed away in January of 1970. Bond hoped that his study of LH's military theories would provide the first "first full-length appraisal of his military thought" and "put LH's military thought in proper

[62] Mearsheimer, ix.

[63] Ibid., 9.

perspective by tracing the origins and development of his principal ideas over his whole career." Arguably, Brian Bond's close relationship with LH allowed him to gain a deeper understanding of LH as a person and provided valuable context.[64]

John J. Mearsheimer, while not a student of LH, "profited greatly from his stimulating writings," but believed that LH's successful personal rebranding post-WWII obscured the true origins and purposes of his military theories. Additionally, Mearsheimer argues that Bond's personal relationship with LH made it difficult for Bond to take a purely objective position throughout his study and therefore Bond's criticisms were not pushed "to their logical conclusion."[65]

By the mid 1920's, LH culminated his analysis of infantry tactics and the principles derived from his "Man in the Dark Theory of War," and refocused his attention on the potential of mechanized warfare. It was at this point LH expanded his intellectual aperture in order to understand war at the operational and strategic levels. LH determined that a rigorous study of history would bring into focus a comprehensive theory of war that would prevent Britain from entering another conflict similar to WWI.[66]

Throughout the interwar years LH advocated in favor of two distinct strategies. The first was armored warfare which prescribed combined arms maneuver to strike the enemy's combat forces in the rear areas. Armored warfare was envisioned as a means to break the defensive stalemate that defined WWI. This concept evolved into what is

[64] Bond, 1-5.

[65] Mearsheimer, x, 16.

[66] Bond, 33, 46.

commonly known as blitzkrieg.[67] The second was the indirect approach, which LH also referred to as deep strategic penetration. The purpose of deep strategic penetration is to avoid an enemy's forces entirely and instead focus the attack on the enemy's civilian population.

Mearsheimer notes that LH first began writing about the importance of armored warfare in the early 1920s after being exposed to the writings of respected British tank commander John Fredrick Charles Fuller. "Fuller firmly believed the tank would be the dominant weapon on future battlefields and, if properly employed, would revolutionize land warfare." However, Mearsheimer notes that, "Liddell Hart often asserted during the 1920s, but not the 1930s, that the tank had the potential to revolutionize land warfare." In fact, Mearsheimer argues that the evidence shows that LH supported mechanization but never fully articulated a blitzkrieg strategy and in reality was still convinced that a strong defense held the advantage. By the late 1920s, LH's writings shifted from armored warfare to a discussion on the merits of the indirect approach, specifically deep strategic penetration.[68]

LH believed that the indirect approach could save Britain from becoming entrenched in another vast conflagration on Continental Europe. Britain's island geography meant that it could, to paraphrase Sir Francis Bacon, take as much or as little of war in Europe as she wanted.[69] LH's experience in WWI convinced him that Britain

[67] Mearsheimer, 6.

[68] Ibid., 33-36.

[69] Julian S. Corbett, *Some Principles of Maritime Strategy* (Annapolis, MD: Naval Institute Press, 1988), 58.

should never again field a large army on Continental Europe. However, "He came to believe that in the event of another war on the Continent, Britain's generals would repeat the experience of the Western Front." It was from this deep-seated conviction that LH launched an impressive campaign promoting a policy of limited liability based on the strategy of the indirect approach. "When Liddell Hart spoke about the indirect approach during the interwar period, he was not talking about blitzkrieg but of finding a way to defeat a Continental foe without having to engage his armies." The indirect approach was built on the belief that the enemy would capitulate if the morale of the civilian population was destroyed. LH argued that the complexity of the modern state created an "Achilles' heel" that could be identified and attacked. LH "believed that if the attacker could 'demoralize one section of the nation, the collapse of its will to resist compels the surrender of the whole." The central purpose of the indirect approach was to propose a different set of options that kept the British off the field of battle on Continental Europe.[70]

As Bond observed, throughout the 1930s, and in reaction to the deteriorating political landscape, LH advocated a British policy of "limited liability."[71] The purpose of limited liability was to prevent British involvement in war on Continental Europe and limit overall involvement to "an air force contingent and naval support."[72] LH wrote extensively in favor of limited liability and emphasized the strength of the defense. LH

[70] Mearsheimer, 85-88.

[71] Bond, 88.

[72] Ibid., 93.

argued that, “The defense is markedly superior to the attack in modern land warfare and that weapon developments actually increase this superiority.”[73] LH pointed to Britain’s geographical position as an island disconnected from Continental Europe and a lack of prior land army preparedness across the range of doctrine, organization, training, materiel, logistics, personnel, and facilities as key reasons to assume a policy of limited liability.[74]

Much of LH’s frustration regarding the conduct of WWI was directed towards the British General Staff; however, he also believed that the prevailing devotion to the Clausewitzian concept of a “decisive battle,” with its emphasis on attrition warfare was equally damaging. “Already by 1924 he had fastened on the notion that Clausewitz was the evil genius whose false strategic doctrine was responsible for futile battles of attrition, such as Verdun, the Somme, and Passchendaele.” Brian Bond argues that LH never altered his opinion of Clausewitz who in, *Paris, or the Future of War* (1925), is referred to as the “Corsican Vampire.” This description referenced Napoleon and argued that Clausewitz’s *On War* was simply a treatise on Napoleonic warfare.[75] Suffice to say LH disagreed fundamentally with a Clausewitzian concept of war emphasizing the decisive

[73] Brian Bond and Martin Alexander, “Liddell Hart and De Gaulle: The Doctrines of Limited Liability and Mobile Defense,” in *Makers of Modern Strategy from Machiavelli to the Nuclear Age*, ed. Peter Paret (Princeton, NJ: Princeton University Press, 1986), 612.

[74] Ibid., 622.

[75] LH felt that Clausewitz’s traumatic experiences during the Napoleonic Wars greatly influenced his theories. LH believed that Clausewitz was simply a man stuck in his era, incapable of understanding warfare enough to objectively distill the most salient lessons. Ironically, LH’s critics argue that his [LH] experiences in WWI directly contributed to his positions on strategy, tactics, and doctrine during the interwar period.

battle and striking directly at the enemy's army. In 1929, his practical and theoretical study converged in, *The Decisive Wars of History*, which contained two essential maxims: "In the face of the overwhelming evidence of history no general is justified in launching his troops to a direct attack upon an enemy firmly in position. Instead of seeking to upset the enemy's equilibrium by one's attack, it must be upset before a real attack is, or can be successfully, launched."[76]

LH derived the maxims to break the "Clausewitzian spell" that had captivated the British military establishment since the Napoleonic era. Prior to official publication LH sent manuscripts to several of his closest peers. The initial feedback clearly indicated that many felt the conceptual framework required refinement. One of the most forceful criticisms came from prominent English military historian, Sir John William Fortescue, who characterized LH's book as "superficial" and "vague on the indirect approach and what is decisive." According to Bond, "Liddell Hart's approach to history was intuitive and eclectic rather than, as he liked to believe, 'scientific'." In addition, Spencer Wilkinson, another respected military historian at Oxford observed that, "Liddell Hart is a little too much the slave of his own theories which he makes into dogmas." The allegation that LH used the book to promote a specific set of military principles is accurate and precisely what LH intended. The book relied on a series of brief historical case studies to argue in favor of LH's derived maxims. The other key criticism is that LH fell into the very trap he attempted to avoid by focusing his analysis on the tactical and operational levels of war "in isolation from their political, social, and economic

[76] Bond, 55.

contexts." In short, "In the Strategy of Indirect Approach he had attempted to formulate an opposing general theory of war to that exemplified in the attrition campaigns of the Western Front."[77]

Mearshiemer remains critical of LH's indirect approach observing that, "The key to understanding the indirect approach is to realize that it is a vague and therefore elastic theory." This elasticity makes it difficult to evaluate the utility or replicate in other studies. Mearshiemer argues that according to LH, "Virtually every military victory can be ascribed to the indirect approach," which amounts to a "circular argument" and not a testable theory. It was precisely this elasticity and LH's command of military history that allowed him to craft a persuasive theory that received support from those within the military and political establishment. However, "his military predictions about the opening battles of the war proved utterly wrong: he totally failed to anticipate the success of the German blitzkrieg." As a result LH's reputation suffered and did not begin to recover until the late 1950s.[78]

In conclusion, it is clear that LH was deeply shaped by his experiences in WWI. Additionally, LH feared that the British General Staff, whom he believed mistakenly placed their trust in Clausewitzian principles, would seek to raise a large land army for use on Continental Europe. LH used his prestige and abilities to develop a broad strategic approach that would persuade decision makers not to devote attention and resources towards creation of a large land army.

[77] Ibid., 33-61.

[78] Mearsheimer, 4, 87.

In the early 1920s, he was interested in mechanized warfare but towards the mid-1920s, and certainly throughout the 1930s, he articulated and proposed the indirect approach. In the aftermath of WWII, LH sought to revive his theory and reputation. He accomplished the former in 1954 by combining mechanized warfare with the indirect approach and retitling his book. Rebuilding his reputation required the remainder of his life.

This study will rely on LH's second revised edition of *Strategy* originally published in 1967 to articulate his Strategy of the Indirect Approach. This edition reflects LH's third and final update and includes everything in the 1954 edition (including his eight principles) but added is an expanded Part III that looks more deeply at Hitler's strategy and a Part IV that incorporates a discussion on strategy and grand strategy. The 1967 edition also includes two appendices, which comprise two letters from successful military commanders (British and Israeli) who provide details on how they relied on LH's principles to achieve success.

In order to articulate his strategy of the indirect approach LH relied on a comprehensive number of case studies spanning an impressive breadth of history beginning with ancient Greece and up through WWII. This breadth of cases limits depth. This fact coupled with LH's command of military history can make it challenging for the student to discern the most salient lessons beyond what LH addresses. As John J. Mearsheimer notes, "although his theories are widely applied today, they were shaped by a unique historical context and should be applied with caution to current security problems."[79] LH developed his comprehensive theory with the intent that it would withstand the test of time and apply to multiple cases across time and distance. However, distilled to its essence, LH's *The Decisive Wars of History* and the subsequent editions were developed in reaction to the British experience in WWI and LH's disapproval of Clausewitzian principles. This study will operationalize LH's eight principles and apply them to cases of cyber conflict. The final insight belongs to Brian Bond whom, while disagreeing with many of LH's historiological methods, provides a compelling reason for LH's continued relevance as a military historian and theorist:

> Whatever its shortcomings from the viewpoint of scholarship, the *Strategy of Indirect Approach* can be strongly defended as an educational doctrine. There was a great deal to be said for encouraging a new generation of officers to think for themselves, and in particular to think in terms of achieving success by surprise and superior mobility; to value intellect and professional skill more than tradition and seniority; and to make the fullest use of science and technology to minimize casualties.[80]

[79] Mearsheimer, ix.

[80] Bond, 59.

CHAPTER 4

METHODOLOGY

> Throughout the ages, effective results in war have rarely been attained unless the approach has had such an indirectness as to ensure the opponent's unreadiness to meet it. The indirectness has usually been physical, and always psychological.
>
> — B.H. Liddell Hart, *Strategy*

This study applies LH's "principles of the indirect approach" to two relevant cyber case studies.[81] The case studies consist of the Stuxnet and Chinese sponsored cyber espionage.[82] Both cases were selected because of their relevance to the overall cyber discussion, and more importantly because each case utilized diverse techniques in pursuit of distinct end states. Additionally, this approach provides LH's principles sufficient breadth to unfold on the analytical canvas. The goal is to understand how, and to what degree, activities in the cyber domain translate to tactical and strategic success, as well as, how LH's principles inform future application.

LH envisioned that his principles would be equally applicable to soldiers on the battlefield and government leaders. In other words applicable at the tactical and strategic level. LH defines strategy as, "The art of distributing and applying military means to fulfill the ends of policy." To this end, "Strategy depends for success, first and most, on a

[81] Liddell Hart, *Strategy*, 334-337.

[82] Stuxnet refers to the 2010 U.S.-Israel cyber attack targeting Iran's nuclear weapons program. Chinese sponsored cyber espionage deals with advanced persistent threats aimed at extracting intellectual property in support of Chinese strategic objectives. Each case study looks at a different aspect of cyber conflict. Stuxnet deals with cyber and its ability to destroy physical infrastructure, while cyber espionage is concerned with information extraction.

sound calculation and coordination of the end and the means." Conversely, LH argues that, "Tactics lies in and fills the province of fighting." LH does not reference the operational level throughout his work and consequentially provides no definition. However, he does identify the linkage between the tactical and strategic levels of war. He argues that, "Strategy not only stops on the frontier, but has for its purpose the reduction of fighting to the slenderest possible proportions." It is important to understand LH's definitions and their anticipated application to correctly actualize his principles.[83]

LH identifies grand strategy as a "higher strategy" developed to "co-ordinate and direct all the resources of a nation, or band of nations, towards the attainment of the political object of the war – the goal defined by fundamental policy." Arguably, LH recognized his most valuable contributions, and convincing arguments bringing about the change he desired, needed to address the strategic vice the tactical level of war.[84]

LH's definitions, while recognizable, do not translate directly to US Department of Defense definitions. For example, Joint Publication 1-02 (JP 1-02) defines the strategic level of war as, "The level of war at which a nation, often as a member of a group of nations, determines national or multinational (alliance or coalition) strategic security objectives and guidance, then develops and uses national resources to achieve those objectives." This definition includes elements of LH's definition of strategy and grand strategy, rendering a clear interchange of terms problematic. Additionally, JP 1-02 defines the tactical level of war as, "The level of war at which battles and engagements

[83] Liddell Hart, *Strategy*, 321-335.

[84] Ibid., 322.

are planned and executed to achieve military objectives assigned to tactical units or task forces." Again, this definition is similar to LH's but not a precise replacement.[85]

Additionally, an analysis blending strategy and tactics necessitates defining the operational level of war, which JP 1-02 defines as, "The level of war at which campaigns and major operations are planned, conducted, and sustained to achieve strategic objectives within theaters or other operational areas."[86] Arguably, the majority of the historical examples supporting LH's indirect approach exists within the spectrum of the operational level of war, with some examples closer to the tactical and some crossing into the strategic.

LH's study sinuously transitions back and forth between tactics and strategy. This fluidity can make it difficult to discern his true meaning. This study will rely on LH's definitions as a means to identify context, but follow-on analysis will rely on current DoD approved definitions as outlined in JP 1-02.

LH explains that the indirect approach, distilled to its essence, is simply an understanding of concentration. In the same vein, LH purports that, "True concentration is the fruit of calculated dispersion." In other words, the true objective in war is to concentrate strength against enemy weakness. This asymmetric matchup is the product of dislocating the enemy and causing him to disperse where he should have concentrated. He notes that the "true aim is not so much to seek battle as to seek a strategic situation so

[85] Joint Chiefs of Staff (JCS), Joint Publication (JP) 1-02, *Department of Defense Military and Associated Terms* (Washington, DC: Government Printing Office, 8 November 2010, as amended through 15 June 2015), 236, 299.

[86] Ibid., 178.

advantageous that if it does not itself produce the decision, its continuation by a battle is sure to achieve this." LH argues that, "the cumulative effect of partial success, or even mere threat, at a number of points may be greater than the effect of complete success at one point."[87] Concentrated strength applied to weakness is designed to dislocate enemy forces both physically and psychologically. This dual-pronged dislocation combines to produce an indirect approach.[88]

Principles of the Indirect Approach

LH identifies eight principles, of which he identifies "six positive and two negative." It was his intent that these "maxims" would operationalize the key themes and provides practitioners a framework informing strategy development and subsequent tactical execution:

1. Adjust your end to your means. LH argues that at certain points it is wise to embark on a strategy of "limited aim." LH notes that the "usual reason for adopting a strategy of limited aim is that of awaiting a change in the balance of force – a change often sought and achieved by draining the enemy's force, weakening him by pricks instead of risking blows." LH argues that the "Fabian strategy" employed by Roman general Fabius against Carthage's Hannibal was, "not merely an evasion of battle to gain

[87] Arguably, this observation, although explained in terms of the indirect approach, is emblematic of LH's "Man in the Dark" concept, which emphasized combined arms maneuver at the platoon level to achieve numerous minor success contributing to a larger, strategic success. It also hints at the possibility of initiating multiple indirect lines of effort to achieve success. This concept is unpacked further in the case study analyzing China-sponsored cyber espionage.

[88] Liddell Hart, *Strategy*, 325-334.

time, but calculated for its effect on the morale of the enemy–and, still more, for its effect on their potential allies." Additionally, LH emphasizes that such an adjustment is not a sign of weakness but demonstrates wisdom and is often necessary to avoid the irrational dedication of resources towards endeavors with little chance to achieve the end state.[89]

2. Keep your object always in mind. "Realize that there are more ways than one of gaining an object." This principle highlights the importance of using the right tool for the job and not becoming unnecessarily wedded to a particular "means." In other words, it is important to ask, what instrument of power will achieve the objective? LH observes that, "Just as the military means is only one of the means to the end of grand strategy – one of the instruments in the surgeons' case–so battle is only one of the means to the end of strategy." Maintaining a clear eye towards the objective relates equally to an economy of force and the creative combination of available means.[90]

3. Choose the line (or course) of least expectation. This principle is concerned with achieving psychological surprise. Operation Overlord is an applicable example. The initial Allied invasion surprised the German General Staff strategically, because the operation was conducted at an unexpected time (during unfavorable weather) and at an unexpected location. Conversely, the Germans were convinced that the Allies would attempt to cross the English Channel at the shortest distance between England and France and prepared a vigorous defense at that location.[91]

[89] Liddell Hart, *Strategy*, 26, 321, 335.

[90] Ibid., 325, 335.

[91] Ibid., 327, 335.

4. Exploit the line of least resistance. This principle relates to the previous but is primarily concerned with achieving physical surprise. LH notes that, "In strategy, the longest way round is often the shortest way home." Meaning that closing with the enemy via a more difficult route requiring maneuver through hazardous terrain (i.e. swamps, forests, mountains, etc.) is preferable to taking an easier more direct route. In the initial action of WWII, the German Army's decision to push mechanized forces through the Ardennes Forrest actualizes this principle. LH notes that, "The Germans . . . in exploiting its possibilities for surprise, had shown their appreciation of the oft taught lesson that natural obstacles are inherently less formidable than human resistance in strong defenses." Another example is found in LH's chapter on the "Roman Wars" which details Hannibal's decision to take the more difficult Etrurian route to attack Flaminius. He notes that Hannibal "ascertained that the other roads leading into Etruria were long and well known to the enemy, but that one which led through the marshes was short, and would bring them upon Flaminius by surprise." Arguably, LH intended this principle to emphasize that movement to the battlefield requires the expenditure of resources and held that expending human energy or fuel, which are replaceable, was more efficient than expending lives. Additionally, pursuing the line of least resistance allows the attacker to select the time and place to make contact with the enemy.[92]

Principles three and four comprise "two faces of the same coin." LH reminds us that, "In studying the physical aspect we must never lose sight of the psychological, and

[92] Liddell Hart, *Strategy*, 5, 25, 217, 335.

only when both are combined is the strategy truly an indirect approach, calculated to dislocate the opponent's balance."[93]

5. Take a line of operation which offers alternative objectives. Arguably, this is LH's most cherished principle and is reemphasized at several points throughout *Strategy*. LH borrows U.S. General William Sherman's famous maxim to illustrate his point, saying a line of operation offering alternative objectives places the "enemy on the horns of a dilemma." The purpose is to force the enemy to be indecisive, dilute his combat power, and fail to concentrate at the correct location. The cumulative effect enables the attacker to move from one objective to another while never facing a numerically superior force. LH believes General Sherman's "March to the Sea" best personifies this principle. Arguing that, "In the physical and moral effect of this deceptive direction lies the only reasonable explanation of his unchecked progress across 425 miles of country strewn with obstacles . . . in the face of an enemy whose numerical strength was ample for effective resistance." Sherman gained an element of surprise and unpredictability by shifting his line of operation off the rail line. This harkens to the previously explained principles. However, Sherman's line of operation included the essential element of threatening several key Confederate cities along his march eastward. This had a profound psychological effect on the enemy, who "became so 'jumpy' that they repeatedly gave way to this moral pressure, and fell back before they felt any serious physical pressure." The various cities in General Sherman's path were either symbolically important or critical to the Confederate war effort. Sherman's lack of reliance on rail made it difficult

[93] Ibid., 327, 335.

for the Confederates to predict his intended path and paralyzed their decision-making. LH reminds his readers that, “A strategist should think in terms of paralyzing, not of killing.” A line of operation threatening alternative objectives grants the attacker flexibility while denying the enemy the same.[94]

6. Ensure that both plan and dispositions are flexible – adaptable to circumstances. This principle is, in many ways, an amalgamation of the previous five. The purpose is to cultivate a flexibility of mind capable of overcoming immediate problems in pursuit of the overall objective. This principle’s underlying concept addresses the dichotomy between concentration and dispersion. Understood this way, LH argues that, “an army should always be so distributed that its parts can aid each other and combine to produce the maximum possible concentration of force at one place, while minimum force necessary is used elsewhere to prepare the success of the concentration.” Arguably, this principle highlights the importance of establishing a military culture that values flexibility and detests rigidity in planning and troop deployment. LH does not explicitly mention military culture as a key component; however, in order for plans and dispositions to achieve the necessary flexibility it is assumed that leaders at every level would be acceptant and expectant that plans would adjust to operational realities.[95]

The previous six principles provided guidance on what to do, and are thus considered positive. The final two principles describe what not to do and are understood as negative.

[94] Liddell Hart, *Strategy*, 135, 212, 330, 335.

[95] Ibid., 328, 336.

7. Do not throw your weight into a stroke whilst your opponent is on guard–whilst he is well placed to parry or evade it. This principle is a reminder to avoid the direct approach. LH notes that, "to move directly on an opponent consolidates his balance, physical and psychological, and by consolidating it increases his resisting power." In other words, a direct strike is where the enemy expects and is prepared to be attacked. In addition to the incorporation of the previous principles, LH cautions, "that a joint is the most sensitive and profitable point of attack, and that a penetration between two forces or units is more dangerous if they are assembled shoulder to shoulder than if they are widely separated and organically separate." This distinction recognizes that the geographical "joint" created when two units (especially if they comprise a multinational force) join their flanks is more vulnerable than two units who are geographically separated and thus responsible for their own flank security. Additionally, LH uses the analogy of a spring that compresses when force is applied directly. The compression makes the spring more "powerful" because it is designed to absorb force in this way. Conversely, a spring pushed from the side simply falls over and ceases to function as a spring.[96]

8. Do not renew an attack along the same line (or in the same form) after it has once failed. This principle actualizes the two maxims central to LH's 1954 edition which were, "no general is justified in launching his troops in a direct attack upon an enemy firmly in position, [and] instead of seeking to upset the enemy's equilibrium by one's attack, it must be upset before the real attack is, or can be successfully launched." Arguably, this principle recalls the British experience in the Great War, which saw

[96] Liddell Hart, *Strategy*, 195, 327, 336.

successive waves of troops sent over no-man’s land in an attempt to break the defensive stalemate. However, in that conflict instead of breaking through enemy defenses hundreds of thousands of British soldiers were killed conducting seemingly illogical frontal assaults. This principle advises commanders not to reinforce failure by committing additional forces to a floundering assault. Additionally, this maxim reiterates the sixth principle, which emphasized that plans and dispositions should be flexible.[97]

It seems clear that LH’s strategy of the indirect approach constitutes a rebuttal of the British experience in the Great War. LH’s principles are explicit and easily understood. However, the application presents difficulties that require identification and mitigation.

However, a key criticism of LH’s historical examples is that, although spanning two millennia, the actions of all the battles, save a handful, were fought on Continental Europe. In this sense, many of his examples could be viewed as an exercise demonstrating the eternality of key terrain.

Additionally, LH’s distinction between strategy and tactics is unclear at several points. LH purports that his principles are applicable at the strategic and grand strategic level, but fall short modern doctrinal definitions. As previously stated, and unless otherwise noted, LH’s principles will be understood to exist along a spectrum from the tactical through strategic level. However, the case studies reveal that tactical actions, especially in the cyber domain, often translate to strategic effects.

[97] Liddell Hart, *Strategy*, 147, 336.

Also potentially problematic is LH’s assumption regarding how these principles verifiably affected the minds of hostile rulers or influenced the psychological state of the enemy. LH’s thesis explicitly states that this is the goal of any strategy but he does not provide any means, vice post-war historical record, to determine if this was achieved in real time. This makes it difficult to determine if such an impact was by design or the result of unintended consequences and the tyranny of events.

CHAPTER 5

STUXNET CASE STUDY

Stuxnet refers to the U.S.-Israel sponsored cyber attack targeting Iranian centrifuges at the nuclear facility in Natanz. Experts assert that this attack is indicative of wider cyber conflict occurring along the fringes of the public consciousness.[98] This perception is owed to Stuxnet's structure and overall objective. In this regard, digital weapons may have opened a "cyber Pandora's box" enabling nations to employ coercive measures in pursuit of national objectives while mitigating the risks associated with conventional weapons. A nation's capacity to conduct discrete operations is especially important when faced with belligerent governments or organizations acting outside international norms. Arguably the cyber domain facilitates the execution of discrete and non-attributable activities.

This chapter analyzes Stuxnet using a case study methodology and applies LH's indirect approach principles. The purpose is to determine if Stuxnet adheres to LH's indirect approach and if the results were decisive. For the purpose of this case study, decisive is defined as an attack's ability to achieve its overall objective, which in this case means destroying Iran's capacity to develop weapons grade uranium, both in terms of physical destruction and national will. Before initiating an analysis it is necessary to establish the key events using the following questions:

[98] Chris Demchak, "Cybered Conflict, Cyber Power, and Security Resilience as Strategy," in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. Derek S. Reveron (Washington, DC: Georgetown University Press, 2012), 122.

1. What made Iran’s nuclear facility at Natanz a desirable target? What characteristics made Natanz targetable?

2. How did Stuxnet carry out its attack (delivery and payload)?

3. Did Stuxnet meet its objective completely or was it discovered before its mission?

4. Why was Stuxnet launched when it was?

Stuxnet was a sophisticated malware amalgamation purpose built to infiltrate Iranian nuclear facilities and attack associated centrifuges. It accomplished this by adjusting the speed at which centrifuges spun thus contaminating the uranium enrichment process. Stuxnet’s genius was its ability to hide this information from unsuspecting Iranian scientists. Stuxnet’s purpose was to deny Iran access to weapons grade uranium.[99] Stuxnet was not a single attack but comprised of three distinct waves. Each new wave was designed to improve upon the former. The first attack was launched in June 2009. Subsequent waves were launched in March and April 2010. Each wave was programed to terminate operations three years from the date of execution. However, on 24 June 2010, Stuxnet was accidentally discovered by a Belarusian cyber security professional who received the malicious code from an antivirus firm based in Iran. This exposure occurred two years earlier than the directed termination date set by Stuxnet’s developers.[100]

[99] Paulo Shakarian, “Stuxnet: Cyberwar Revolution in Military Affairs,” *Small Wars Journal* (15 April 2011): 2-3.

[100] Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World’s First Digital Weapon* (New York: Crown Publishers, 2014), 5-24.

Iran Nuclear Development

Iran's resolute commitment to nuclear development began in 1988. It had been a decade since Ayatollah Ruhollah Khomeini had driven the Shah from power and nearly four decades since the Shah signed the nuclear cooperation agreement in 1954. Initially, Khomeini vehemently opposed restarting Iran's nuclear program because of the technology's association with the West. However, Khomeini modified this view in the wake of the Iran-Iraq War and initiated construction at the Bushehr facility; the site originally developed by the Shah. Iran was unable to develop a nuclear capability unilaterally. After futile attempts to tap the capabilities of nuclear nations Iran's leadership approached Pakistan's Abdul Qadeer Khan, also known as the "father of Pakistan's atomic bomb." Khan, a prolific scientist and businessman, had reasons besides scientific freedom or financial compensation to assist the Iranians. According to Khan, "Iran was an important Muslim country . . . If Iran succeeds in acquiring nuclear technology, we will be a strong bloc in the region to counter international pressure. Iran's nuclear capability will neutralize Israel's power." Over the next two decades, Iran leveraged Khan's scientific knowledge and vast network to import key components to develop weapons grade uranium.[101]

On 14 August 2002, the National Council of Resistance of Iran, "a coalition of Iranian opposition groups in exile . . . announced that Iran was building an illicit nuclear facility near Natanz." Alirerza Jafarzadeh, the group's spokesman, revealed the location

[101] Erich Follath and Holger Stark, "The Birth of a Bomb: A History of Iran's Nuclear Ambitions," *Spiegel Online*, 17 June 2010, accessed 2 February 2016, http://www.spiegel.de/international/world/the-birth-of-a-bomb-a-history-of-iran-s-nuclear-ambitions-a-701109.html.

and purpose of two “secret nuclear programs” that existed outside the “knowledge of the International Atomic Energy Agency [IAEA].” It is speculated that Israeli intelligence services provided the National Council of Resistance of Iran with the information in order to increase the legitimacy of the claims and raise public awareness.[102]

In February 2003, Iranian President Sayyid Mohammad Khatami “acknowledged that Iran was building a uranium enrichment plant at Natanz” and authorized inspectors from the IAEA to visit the site. The inspectors noted the centrifuges resembled IR-1s of an “early generation Urenco design.” At the time, it was unknown how Iran procured the centrifuges. “Centrifuges are metal cylinders with rotors inside that can spin at speeds in excess of 100,000 revolutions per minute to enrich uranium hexafluoride gas.” They are a critical component within any nuclear facility and manufactured by a select handful of companies. Soon after the visit inspectors put the pieces together and determined that Khan provided Iran with designs he stole while working at Urenco.[103]

The IAEA continued to press the Iranians for transparency. However, the Iranian Government continued to propagate statements interlaced with deceptive half-truths accentuating its defiance towards IAEA inspectors, and the West in particular. Ahmadinejad, elected in 2005, signaled a change in Iranian attitudes towards the West—for the worst. Iran’s policies and rhetoric elevated fears in the United States and Israel of a nuclear Iran. Ariel (Eli) Levite, former deputy director general of the Israel Atomic Energy Commission commented that, “Iran didn’t actually have to build a

[102] Zetter, *Countdown to Zero Day*, 34.

[103] Ibid., 47-73.

nuclear weapon to be a threat. All it had to do was master the enrichment process and produce enough low-enriched uranium to make a bomb should it choose to." Iran continued to outfit secret nuclear facilities with centrifuges and continued to improve their enrichment processes. Israel feared that the Iranian "nuclear issue" would become entrenched if Iran mastered this process and was able to conduct industrial scale enrichment.[104]

In May of 2006, "Iranian officials announced that technicians at the pilot enrichment plant at Natanz had succeeded in enriching their first batch of uranium to 3.5 percent, using a full cascade of 164 centrifuges." For Iran watchers in the United States and Israel, this was an alarming development because it signaled that the passage of time was the only variable preventing procurement of weapons grade uranium. The IAEA promptly "declared Iran in noncompliance with its safeguards agreement after years of being urged to do so by the United States." The United Nations followed suit and adopted economic sanctions against Iran.[105]

IAEA experts, Olli Heinonen and Mohamed ElBaradei, along with experts across the international intelligence community acknowledged Iran was enriching uranium. However, each held a different opinion regarding the existence of an Iranian nuclear weapons program. This ensured the situation remained ambiguous. The discrepancy came into sharp contrast when the 2007 *National Intelligence Estimate* (NIE) stated with conviction that, "We [United States intelligence communities] judge with high

[104] Zetter, *Countdown to Zero Day*, 82.

[105] Ibid., 83.

confidence that in Fall 2003, Tehran halted its nuclear weapons program."[106] The NIE is an important document and is intended to shape priorities and resource allocation at the national level. It is delivered to the president and includes the most salient intelligence reports. The persuasive strength of the NIE is based on the collaborative collation and high degree of group concurrence. The 2007 NIE conflicted with multiple Israeli reports and those of other nuclear experts, making it difficult for the United States and Israel to agree on a course of action.

In 2008, Olli Heinonen, the IAEA's deputy director general, convened a secret meeting for thirty-five diplomats in Vienna (represented nations included the United States, Israel, and Iran) in order to discuss the extent of Iran's nuclear program. Heinonen described in detail Iran's secret projects to extract uranium, test explosive nuclear material, and develop a warhead for their Shahab-3 missile. The briefing included pictures of facilities, key documents, and important contact lists all obtained through covert means and passed to the IAEA. The IAEA considered this clear evidence of an Iranian nuclear weapons program, but there remained disagreements on what steps the international community should take beyond economic sanctions. [107]

In summary, since the end of the Iran-Iraq War in 1988 the Iranian Government, under the initial direction of Ayatollah Khomeini, has made the development of nuclear weapons a key national priority.[108] The Iranians were able to procure the required nuclear

[106] Follath and Stark, "The Birth of a Bomb: A History of Iran's Nuclear Ambitions," 9.

[107] Ibid., 1.

[108] Follath and Stark, 3; Iran Watch, "A History of Iran's Nuclear Program," 1 March 2012, accessed 8 January 2016, http://www.iranwatch.org/our-publications/

infrastructure through Abdul Qadeer Khan. Over the years, discrepancies within the international community regarding the true nature of Iran's nuclear ambitions and the difficulty obtaining undeniable evidence limited available options.

Stuxnet Attacks!

This section discusses the strategic environment immediately preceding the employment of Stuxnet. The previous discussion highlighted Iran's nuclear program trajectory and argued that intelligence gaps and differing conclusions made it increasingly difficult for the United States and United Nations to pursue a unified response beyond economic sanctions. However, there are two principle reasons the United States and Israel did not conduct unilateral or bilateral conventional strikes against Iranian nuclear facilities. First, the United States was engaged in two major land wars geographically buttressing Iran's borders, Iraq and Afghanistan. Second, Israel lacked the ability to conduct an aerial attack without crossing significant distances through adversarial air space, sacrificing surprise, and increasing risk.

In 1981 and 2007, the Israeli Air Force conducted successful air strikes destroying nuclear facilities in Iraq and Syria, respectively. However, in both cases the air force attacked a "single, aboveground facility that was not heavily fortified, and in the case of Syria, the target was close enough to home that pilots could make their strike quickly and return before the Syrians had time to respond." Iran learned that consolidated

weapon-program-background-report/history-irans-nuclear-program; Iran Watch, "Iran Nuclear Milestones: 1967-2013," 1 June 2013, accessed 8 January 2016, http://www.iranwatch.org/our-publications/weapon-program-background-report/iran-nuclear-milestones-1967-2013.

aboveground facilities were vulnerable to airstrikes and thus adopted a policy of dispersed, subterranean infrastructure. Israeli intelligence would have difficulty identifying all of Iran's nuclear facilities, while Israeli pilots, flying through contested airspace, would sacrifice the element of surprise and severely jeopardize mission accomplishment. Consequently, the risk associated with a conventional aerial attack exceeded acceptable limits.[109]

There are five reasons why a cyber attack aimed at destroying, or at least damaging, Iran's nuclear infrastructure made strategic sense. First, "slowing the country's rapid race to nuclear breakout . . . would relieve some of the pressure on diplomatic efforts." Second, U.S. and Israeli officials hoped that an undetectable attack would create internal frustration ultimately fracturing political ties within the Iranian regime. Third, lack of high confidence attribution would blunt an acceptable Iranian response. Fourth, it was believed that destroying Iran's nuclear supplies would curtail their enrichment process. Fifth, unlike a conventional attack, a well-executed cyber attack can penetrate both known and unknown facilities. This capability was especially important due to Iran's strategy of infrastructure dispersion and fortification.[110]

[109] Zetter, *Countdown to Zero Day,* 192-193; Erich Follath and Holger Stark, "The Story of 'Operation Orchard': How Israel Destroyed Syria's Al Kibar Nuclear Reactor," *Speigel Online,* 2 November 2009, accessed 9 February 2016, http://www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663.html.

[110] Zetter, *Countdown to Zero Day,* 195-196; David E. Sanger, "US Rejected Aid for Israeli Raid on Iranian Nuclear Site," *New York Times,* 10 January 2009, accessed 26 April 2016, http://www.nytimes.com/2009/01/11/washington/11iran.html?_r=0; William Broad, John Markoff, and David E. Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," *New York Times,* 15 January 2011, accessed 11 February 2016, http://www.nytimes.com/2011/01/16/world/middleast/16stuxnet.html?_r=1.

Stuxnet, like most digital weapons consists of two parts, a delivery system and the payload. Similar to conventional weapons, the delivery system takes the payload to the target. In digital weapons, the payload constitutes the malicious code, and in this case was designed to alter the rotating speeds of the centrifuges by interacting with the attached Programmable Logic Controllers (PLCs). Stuxnet's functionality reflects the deliberate decision-making behind the attack. For example, Stuxnet attacked a specific version of centrifuge, arrayed in a specific cascade, and spinning at a specific speed. This specificity indicates substantial prior knowledge, both technical and of the intelligence variety.[111]

Additionally, Stuxnet's sheer size and complexity bewildered cyber experts. In the weeks after Stuxnet exposure top researchers at the Department of Homeland Security reverse engineered the malware and "catalogued some 4,000 functions in the code—more than most commercial software packages contained."[112] It was later determined that Stuxnet employed five zero day exploits. Additionally, uncompressed Stuxnet was 1.18 megabytes.[113] The level of sophistication indicated that it was developed by a nation state.[114] In 2012, U.S. officials speaking on the condition of anonymity acknowledged

[111] Zetter, *Countdown to Zero Day,* 52.

[112] Ibid., 187.

[113] Ibid., 24.

[114] Nicolas Falliere, Liam O. Murchu and Eric Chien, *Symantec Security Response, W32.Stuxnet Dossier: Version 1.4* (Cupertino, CA: Symantec Corporation, February 2011), 55.

that Stuxnet was a combined U.S.-Israel venture and was part of a much larger cyber campaign targeting Iran's nuclear development.[115]

Antivirus researchers assess that Stuxnet was the work of three separate teams. "One was an elite, highly skilled tiger team that worked the payload . . . a second tier team [was] responsible for the spreading and installation mechanisms . . . and a third team, the least skilled of the bunch, set up the command-and-control servers and handled the encryption and protocol for Stuxnet's communication." This indicates that developing Stuxnet was a large undertaking requiring significant resources at a national level, both technical expertise, and not the work of a disparate group of "hacktivists."[116]

Zero day exploits "are the hacking world's most prized possession because they attack holes that are still unknown to the software maker and to the antivirus vendors." Stuxnet included five such exploits, one of which made Stuxnet invisible to antivirus machines. Consequently, millions of computers running a Windows operating system became infected. One of Stuxnet's core strengths, which also turned out to be its Achilles heel, was its ability to spread. Additionally, Stuxnet contained "eight different propagation methods," none of which relied on Internet access. The developers knew that accessing the deepest recesses of an Iranian nuclear facility would require "someone carrying the infection from one machine to another via a USB flash drive or, once on a machine, via local network connection." The number of zero days and propagation

[115] Ellen Nakashima and Joby Warrick, "Stuxnet Was Work of US and Israeli Experts, Officials Say," *The Washington Post*, 2 June 2012, accessed 27 April 2016, https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html.

[116] Zetter, *Countdown to Zero Day,* 64, 178.

techniques demonstrates that Stuxnet's developers had tremendous resources at their disposal and simply selected those most applicable for the job.[117]

One of Stuxnet's greatest strengths was its use of legitimate digital certificates. "Certificate authorities are the core of trust relationship that makes the Internet function." Built on complex cryptographic concepts, digital certificates are only distributed to vetted companies, which are typically protected on offline servers. Stuxnet procured valid digital certificates from two different companies. Software developers and anti-virus firms rely on digital certificates to sign products and verify authenticity. "Computers assume that a file signed with a legitimate digital certificate is trustworthy." Stuxnet's use of digital certificates enabled the malware to walk through the front door of the targeted computer systems.[118]

To ensure Stuxnet reached Natanz initial salvos were launched against five Iranian companies. These companies were involved with "industrial control and processing of some sort . . . [and] they had some connection to Natanz as contractors." Once on a system, "Stuxnet determined if the computer was a 32-bit or 64-bit Windows machine; Stuxnet only worked with 32-bit Windows machines." It was expected that once inside these companies Stuxnet would infiltrate Natanz via a USB device or an infected computer connected to the local network. Antivirus researcher Symantec

[117] Zetter, *Countdown to Zero Day,* 6, 91-92; Falliere, Murchu, and Chien, 48; Shakarian, 6.

[118] Zetter, *Countdown to Zero Day,* 11-12, 262; Shakarian, 7; Costin G. Raiu and Alex Gostev, "A Tale of Stolen Certificates," *Secureview* (2011): 6-10.

"counted 12,000 infections at these five targets, and from these initial victims Stuxnet then spread to more than 100,000 machines in more than 100 countries."[119]

Stuxnet specifically "looked for a plant that had up to 186 of the [frequency] converters installed, all of them operating above 800Hz." This configuration and corresponding operating speed indicated uranium enrichment in support of a nuclear weapons program. Once Stuxnet accessed Natanz it remained on the facility's local area network until it was transported to a Siemen PLC controlling the centrifuges. PLCs are small computers that are attached to each centrifuge. These devices allow researchers to monitor the status of centrifuge and make changes. The Natanz centrifuges were air gapped from the network, however, it was necessary for researchers and technicians to periodically read and write on the PLCs. To do this they needed to connect a USB device or computer to the PLC.[120]

Once Stuxnet confirmed it had reached a nuclear facility, it located computers that contained SIMANTIC Step 7 software or the SIMATIC WinCC program. "Both programs are part of an industrial control system (ICS) designed to work with Siemens PLCs." Stuxnet was only concerned with specifically configured S7-315 and S7-417 PLCs. "The configuration Stuxnet was looking . . . was likely to be found in only a single facility in Iran or, if more than one, then facilities configured exactly the same, to control an identical process." The delivery system targeting S7-417 PLCs searched for a grouping of "984 devices configured into six groups of 164." Even more specifically it

[119] Zetter, *Countdown to Zero Day,* 60, 92, 97, 338; Shakarian, 5; Falliere, Murchu, and Chien, 3, 4 7, 13 16.

[120] Zetter, *Countdown to Zero Day,* 234; Shakarian, 2, 3.

sought systems labeled A21-A28. Stuxnet’s delivery system was a carefully crafted creation infused with a complex algorithm necessary to achieve positive target identification. Unfortunately, Stuxnet’s final versions were so adept at spreading that they infected computers well beyond the initial target set.[121]

The payload executed differently depending on if the target was a 315 or a 417 PLC. When the delivery system reached a 317 it conducted a reconnaissance phase lasting approximately thirteen days. During this period “Stuxnet sat silently on the PLC recording normal operations in order to loop the data back to operators when the sabotage began.” In other words, the initial phase allowed Stuxnet to gather data regarding the normal functioning of the PLC and repeat this data back after the attack began. This ensured researchers would remain oblivious to the destruction taking place. Stuxnet also prevented researchers from reprogramming the PLC, interfering with Stuxnet’s operation or seeing any error messages. Next, Stuxnet initiated a two-hour countdown after which time a fifteen-minute period of sabotage began. Once complete, the cycle restarted with a twenty-six-day reconnaissance period followed by a fifty-minute attack. Again, repeating a cycle of reconnaissance and attack. During the attack phase “the frequency of the converters [was increased] to 1,410 Hz . . . then reduced to 1,064 Hz.” The purpose was not to damage the PLC or centrifuges but to render the uranium unusable.[122]

[121] Zetter, *Countdown to Zero Day,* 17, 175, 237, 303; Shakarian 2, 3, 5; Falliere, Murchu, and Chien, 12, 26.

[122] Zetter, *Countdown to Zero Day,* 123-24, 231, 235; Shakarian, 2-5; Falliere, Murchu, and Chien, 41-47.

It was assessed that the 2009 version of Stuxnet unsuccessfully targeted only the 417, while the two 2010 iterations switched focus to the 315 and included updated malware for the 417. Additionally, Stuxnet's approach to 417 PLCs was slightly different. The 417 is a higher quality PLC costing around $10,000 vice $500 for a 315. Initially, the payload targeting 417s was concerned with "targeting the valves that managed the flow of uranium hexafluoride gas into and out of the centrifuges and cascades at Natanz." The anticipated result would be an over pressurization of the centrifuge destabilizing the equipment. However, this tactic was likely unsuccessful and later versions of Stuxnet switched to targeting the frequency converters, which was an easier way to manipulate the spinning centrifuges.[123]

Was Stuxnet Successful?

Did Stuxnet achieve its mission? One observer from the press noted that, "Code analysis makes it clear that Stuxnet is not about sending a message or proving a concept . . . it is about destroying its target with utmost determination in military style."[124] Stuxnet successfully infiltrated the Natanz nuclear facility and damaged hundreds of centrifuges. However, "If Stuxnet's goal was the destruction of all the centrifuges [at Natanz] then it had certainly failed."[125] Arguably, what Stuxnet did do was buy time for diplomacy to take effect and "temporarily slowed down Iran's rate of

[123] Zetter, *Countdown to Zero Day,* 236, 303; Shakarian, 2-4; Falliere, Murchu, and Chien, 36-38.

[124] Broad, Markoff, and Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay."

[125] Zetter, *Countdown to Zero Day,* 359.

expansion."[126] Stuxnet did destroy several tons of uranium gas and their finite supply of centrifuges. However, it is reported that during this period Iran increased its "production of low-enriched uranium" from 2010 onwards.[127] While there are certainly valid criticisms regarding Stuxnet's slow and incremental approach it can also be argued that it made it more difficult for Iran "to make a case for striking back" and might have prevented Israel from conducting a unilateral conventional strike.[128] However, several experts conclude that Stuxnet was released too early and should have been delayed until Iran had installed more centrifuges.[129] This would have allowed Stuxnet to strike nuclear facilities operating at full capacity, which would have had a greater cumulative effect. Ultimately, Stuxnet was discovered and Iran took all its centrifuges offline in order to wipe the malware.

Also of note were assassination attempts against prominent Iranian scientists in the weeks and months following Stuxnet's shutdown. Two of the attacks succeeded in killing Mostafa Ahmadi Roshan, the Natanz's facility manager, and Majid Shahriari, an important nuclear scientist.[130]

[126] Ibid., 361.

[127] Eli Lake, "Operation Sabotage," *New Republic* (13 July 2010): 5, accessed 22 February 2016, https://newrepublic.com/article/75952/operation-sabotage.

[128] Zetter, *Countdown to Zero Day,* 365, 369.

[129] Ibid., 365.

[130] Saeed Kamali Dehghan and Julian Borger, "Iranian Nuclear Chemist Killed By Motorbike Assassins," *The Guardian,* 11 January 2012, accessed 22 February 2016, http://www.theguardian.com/world/2012/jan/11/iran-nuclear-chemist-killed; BBC News, "Iranian Nuclear Scientist Killed in Motorbike Attack," *BBC,* 29 November 2010, accessed 12 February 2016, http://www.bbc.com/news/world-middle-east-11860928; William Yong and Robert Worth, "Bombings Hit Atomic Experts in Iran Streets," *The*

Stuxnet's "biggest payoff . . . may not come from the sabotage itself, but from the psychological effect it could have on Iran's government" in terms of "keeping Iranian officials paranoid and off-balance." However, it is clear that neither Stuxnet nor the targeted assassinations stopped Iran's uranium enrichment program. Henry Sokolski, the executive director of the Nonproliferation Policy Education Center, argues that "sabotage is helpful, but not [successful] on its own and [certainly] not as a substitute for sound policy."[131]

LH's Indirect Approach Principles

Stuxnet overwhelmingly adhered to LH's indirect approach principles with one exception. We can now discuss the points of convergence and divergence. The eight principles are: (1) adjust your end to your means; (2) keep your object always in mind; (3) choose the line (or course) of least expectation; (4) exploit the line of least resistance; (5) take a line of operation which offers alternative objectives; (6) ensure that both plan and dispositions are flexible**—**adaptable to circumstances; (7) **d**o not throw your weight into a stroke whilst your opponent is on guard**—**whilst he is well placed to parry or evade it; and (8) do not renew an attack along the same line (or in the same form) after it has once failed. A detailed explanation of each principle is contained in chapter 4 (methodology).

New York Times, 29 November 2010, accessed 12 February 2016, http://www.nytimes.com/2010/11/30/world/middleast/30tehran.html?_r=0.

[131] Lake, 6-7.

Adjust ends to means, refers to embracing a strategy of limited aim in order to await a favorable shift in balance. Stuxnet afforded the United States the ability to take action against Iran's nuclear program without risking a conventional retaliation. The United States was engaged in two large-scale land wars adjacent to Iran and could ill afford to open a third front. Additionally, U.S. decision makers were under increasing pressure from their Israeli counterparts to stop Iran militarily, or at least grant Israel permission to strike. The United States understood that time was running out to disrupt Iran's nuclear program but a conventional strike was out of the question and imposed economic sanctions were not likely to collapse Iranian will. In other words, Stuxnet slowed down Iran's overall nuclear efforts and temporarily disrupted their progress, thus granting maneuver space for other instruments of national power such as diplomacy and economic sanctions. For these reasons Stuxnet does adhere to this principle.

Keeping the object always in mind, highlights that accomplishing the objective is more important than the means employed. This principle does not advocate a Machiavellian approach where the ends always justify the means, but is meant to reinforce the importance of maintaining flexibility of mind in the selection and employment of the means. Decision makers determined that their options was not a simple choice between a conventional strike and doing nothing, but included a repertoire of possible actions. Arguably, Stuxnet was one of several possibilities presented to decision makers. The reason for rejecting the others is not known, but it does indicate that Stuxnet was the course of action that optimized risk versus reward. The vast collaboration across disciplines and expertise between the United States and Israel suggests that at the point of execution, both countries locked step towards a clear objective. As the case study mentioned, multiple teams were required to compile and deliver Stuxnet’s malware. For these reasons Stuxnet does adhere to this principle.

Choosing the line (or course) of least expectation, is concerned with achieving psychological surprise. Stuxnet’s payload was specifically designed to avoid detection throughout the operation. This was necessary to carry out the attack and to foment internal angst within Iranian leadership. It accomplished this by subtly sabotaging the centrifuges while ensuring the associated PLCs reported normal operating parameters. Iranian researchers were unable to determine the cause of the failures. Were they sold faulty equipment? Did one of their colleagues betray them? The inability to identify and isolate the problem until an outside antivirus company discovered the code demonstrates that Stuxnet would have continued to be a source of speculation and intrigue within the Iranian nuclear establishment. For these reasons Stuxnet does adhere to this principle.

Exploiting the line of least resistance**,** seeks to achieve physical surprise. Iran learned from Iraq and Syria that consolidated and aboveground nuclear facilities are susceptible to aerial attacks. To overcome this vulnerability Iran employed a strategy of dispersion and fortified subterranean complexes. Arguably, Iran was confident that Western governments lacked the intelligence capabilities and military hardware necessary to identify and strike the many belowground nuclear facilities. This was a valid assumption. The Western intelligence community knew of Natanz at least since 2002 and IAEA inspectors visited this site along with several others. However, the existence and progress of unknown sites caused the greatest anxiety. Western intelligence agencies knew conclusively that there were companies with access to Iran’s nuclear sites. Therefore, Stuxnet was programmed to spread quickly but only attack specific targets.

This capability ensured that the malware would end up in a nuclear facility regardless if it was previously known or not. Likewise, secrecy, fortification, and air-gapped systems were irrelevant. Stuxnet did not take the most direct route to its intended target but instead pursued a line of operation guaranteeing access. For these reasons Stuxnet does adhere to this principle.

Taking a line of operation, which offers alternative objectives, emphasizes putting the enemy on the "horns of a dilemma" by forcing the enemy to dilute their combat power and safeguard multiple vulnerable locations. Executed correctly, an enemy's decision making is paralyzed. Stuxnet was purposely extremely specific. It was built to manipulate either S7-315 or S7-417 PLCs, ultimately sabotaging uranium enrichment efforts. In fact, if Stuxnet found itself on a machine without the required Siemens software it sat dormant until it reached a new machine and then queried the system for its specifications. However, "Stuxnet was just one in an arsenal of tools the attackers had used against Iran and other targets."[132] Additionally, it is acknowledged that Stuxnet comprised a small piece of a much larger cyber campaign.[133] It is possible that at the strategic level it was discussed that if Stuxnet failed other courses of action would be executed; however, this is largely unknown and beyond the scope of this study. Additionally, it is entirely reasonable to assume that the assassinations of principal Iranian scientists constituted an entirely separate line of effort and was not necessarily the

[132] Zetter, *Countdown to Zero Day*, 249.

[133] Nakashima and Warrick.

result of Stuxnet’s exposure, or even associated with the United States. For these reasons Stuxnet does not adhere to this principle.

Ensuring that both plans and dispositions are flexible—adaptable to circumstances, discusses the importance of promoting a flexibility of mind that allows planners and decision makers to adapt their approach to the actual situation. In many ways this principle succinctly captures the essence of the previous five. After Stuxnet infected a system, it logged the IP address, the version of Windows, and reported if it found a system with the targeted Siemens software installed. Next, it sent this information back to command servers located in Denmark and Malaysia. This allowed Stuxnet’s handlers to determine if the malware reached its intended target. It also allowed developers to tweak the code and make it more effective. This is most likely the reason Stuxnet was released in three distinct waves, each containing minor adjustments. It was observed that the final version of Stuxnet contained the most aggressive “spreading power.” Additionally, the code targeting S7-417 PLCs switched from manipulating the “flow of uranium hexafluoride gas into and out of the centrifuges” to attacking frequency converters. Arguably, this was accomplished after reviewing the information sent to the command servers. For these reasons Stuxnet does adhere to this principle.[134]

Do not throw your weight into a stroke whilst your opponent is on guard—whilst he is well placed to parry or evade it, advises not to strike in a way that reinforces an enemy’s strengths or consolidates his defenses. This was Stuxnet’s strength. Iran took steps to mitigate an aerial attack and used the international stage to emphasize their legal

[134] Zetter, *Countdown to Zero Day*, 27-28, 96, 303.

and peaceful pursuit of nuclear power. Disagreements between experts and nations regarding Iran's true intentions made it difficult to unequivocally counter their narrative. Even with clear evidence it was still up to the individual decision maker to draw a conclusion. However, Iran was not prepared to defend every function of their nuclear facilities. Physical security and air-gapped systems formed the foundation. Stuxnet defeated both. Additionally, Stuxnet's incremental nature disarmed a conventional response. Stuxnet's "slow and stealthy attack was a compromise of sorts that made it harder to achieve more decisive results but also made it harder for Iran to make a case for striking back."[135] Iran could not evade or parry Stuxnet as long as it remained undiscovered. For these reasons Stuxnet does adhere to this principle.

Do not renew an attack along the same line (or in the same form) after it has once failed, cautions decision makers not to commit additional resources to a failed operation without reassessing the operational variables and employing a different approach. Arguably, this is a fundamental principle within the cyber community. It is understood that once an attack is conducted the exact construct and zero days utilized are no longer acceptable. Software developers and companies will patch their systems and cybersecurity professionals will add the malware to their antivirus database. Additionally, in many cases, "A cyberweapon [is] the type of weapon that you fire and it doesn't die. Somebody can pick it up and fire right back at you."[136] This perspective stresses that, given enough time, even the most complex cyber attacks can be analyzed and

[135] Zetter, *Countdown to Zero Day*, 365.

[136] Ibid., 210.

repackaged. Once Symantec exposed Stuxnet, the command and control servers managing the attack went silent and Iran took all centrifuges offline.[137] For these reasons Stuxnet does adhere to this principle.

Conclusion

In conclusion, Stuxnet adhered to seven of eight principles and overall conforms to LH's indirect approach. However, the results were far from decisive. It is possible to argue that Stuxnet allowed future diplomatic efforts to succeed. It is equally possible to claim that Stuxnet was a failure. If Stuxnet were able to threaten alternative objectives would it have achieved decisive results? It is difficult determine how this would have improved Stuxnet in a meaningful way without drastically changing a key variable in the decision calculus. Arguably, Stuxnet would have avoided detection for a much longer period, if the developers restricted the malware's capacity to spread. Although Stuxnet did not release its payload unless it found itself on a targeted system, the delivery method caused infected machines to crash continuously.

Stuxnet also showed that for an offensive cyber attack to succeed the attackers must know a great deal about the targeted systems. It is not enough to know the geographical location, information which may not even be necessary. However, malware developers need to know every aspect of the targeted systems. This level of fidelity takes time to obtain. Additionally, once this information is known experts must construct the cyber tools enabling success. All of this requires practicing on systems mimicking the actual configuration. This ensures the code runs as intended and provides opportunities to

[137] Ibid., 128, 238.

implant branch attacks. A successful cyber attack capable of penetrating and destroying industrial control systems, especially within nuclear facilities, requires time and the partnership and input of experts across a variety of disciplines.

CHAPTER 6

CHINESE CYBER ESPIONAGE CASE STUDY

Over the past decade, Chinese-sponsored cyber intrusions against U.S. industries and government systems number in the tens of thousands. The sheer volume has led to the adoption of various monikers such as Operation Aurora, Titan Rain, Byzantine Hades, GhostNet, Shady RAT, and Comment Crew/Group. Each label refers specifically to advanced persistent threats stemming from Chinese sanctioned cyber espionage. In fact, “much has been written within China on the subject of cyberwarfare. By contrast virtually nothing has appeared in print on the subject of cyber exploitation (i.e. cyber espionage).”[138] Throughout this case study the terms “China” and “Chinese” refer to the People’s Republic of China (PRC) in general and the Chinese Communist Party (CCP) in particular. The term “Chinese military” always refers to the People’s Liberation Army (PLA).

This case study analyzes Chinese cyber espionage in order to understand the strategic underpinnings and methods. The purpose is to gain insight into the overall objectives and apply LH’s indirect approach principles. The case study begins with a general orientation to Chinese cyber espionage and moves into a historical discussion before addressing the deeper strategic principles informing China’s cyber approach. Next is a discussion of APT techniques aimed at addressing what they are, and how they work.

[138] Nigel Inkster, “The Chinese Intelligence Agencies: Evolution and Empowerment in Cyberspace,” in *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, ed. Jon R. Lindsay, Tai Ming Cheung, Derek S. Reveron (New York: Oxford University Press, 2015), 42.

Lastly, the case study applies LH's indirect approach principles to China's cyber espionage. This case study seeks to answer the following:

1. Why is Chinese cyber espionage so pervasive?

2. What strategic underpinnings inform China's reliance on cyber espionage?

3. Does China's use of cyber espionage constitute an indirect approach? Would the Chinese agree?

4. What can be done to mitigate China's cyber espionage capabilities?

Recent History

In 2005, U.S. officials publicly acknowledged that over the past three years government information networks faced a relentless onslaught of attempted cyber intrusions traced to China. U.S. investigators referred to this cyber campaign as Titan Rain.[139] However, it remained unclear if the intrusions reflected a "coordinated Chinese government campaign" or if they were "the work of other hackers simply using Chinese networks to disguise the origins of the attacks."[140] U.S. decision makers sought additional data points in order to clearly identify linkages to the Chinese Government.

In 2007, British news outlets published an article linking Chinese cyber hackers to attacks against British Government departments including the Ministry of Defense and House of Commons. The same article noted that computers associated with Germany's,

[139] Bradley Graham, "Hackers Attack Via Chinese Web Sites," *The Washington Post*, 25 August 2005, accessed 5 April 2016, http://www.washingtonpost.com/wp-dyn/content/article/2005/08/24/AR2005082402318.html.

[140] Ibid.

Angela Merkel, were the target of Chinese based cyber attacks.[141] Additionally, throughout 2007 Chinese based cyber attackers sent over 1,000 emails to a U.S. nuclear weapons laboratory with the intent of accessing their networks.[142]

In 2009, several media outlets covered stories that described the severity of Chinese and Russian based cyber attacks launched against the U.S. electrical grid. The purpose of the attacks was not to destroy critical infrastructure but, to map the systems and plant "software tools" that could be used to "destroy infrastructure components." The article noted that, "The growing reliance of utilities on Internet-based communication has increased the vulnerability of control systems to spies and hackers." However, U.S. efforts to identify a clear link between the attackers and the Chinese Government remained elusive.[143]

In 2011, *The Washington Post* published an article outlining the extent of China's cyber attacks, mentioning the complex attack against Google dubbed Operation Aurora and several others. The article noted that a single server linked to China was responsible for "hacking more than 70 corporations and government organizations." James A. Lewis, a cybersecurity expert at the Center of Strategic and International Studies, acknowledged

[141] Richard Norton-Taylor, "Titan Rain–How Chinese Hackers Targeted Whitehall," *The Guardian,* 4 September 2007, accessed 5 April 2016, https://www.theguardian.com/technology/2007/sep/04/news.internet.

[142] John Markoff, "Cyber Attack on US Nuclear Arms Lab Linked to China," *The New York Times,* 9 November 2007, accessed 5 April 2016, http://www.nytimes.com/ 2007/12/09/world/americas/09iht-hack.1.8653712.html?_r=0.

[143] Siobhan Gorman, "Electricity Grid in US Penetrated by Spies," *The Wall Street Journal,* 8 April 2009, accessed 5 April 2016, http://www.wsj.com/articles/ SB123914805204099085.

that Chinese based cyber intrusions have been occurring since at least 1998 and cybersecurity expert John McAfee coined the term Operation Shady RAT to describe the phenomenon. McAfee's vice president reported that, "We're facing a massive transfer of wealth in the form of intellectual property that is unprecedented in history." While attacks are directed against a multitude of government and business cyber networks, Scott Borg, the chief economist at U.S. Cyber Consequences Unit, "assessed the annual loss of intellectual property and investment opportunities across all industries at $6 billion to $20 billion, with a big part owning to oil industry losses." Cyber attacks against the oil industry are compelling because this industry deals in nonrenewable resources that must be located and extracted, usually within sovereign territory or a country's exclusive economic zone.[144] This requires a substantial investment in research in order to assess potential profits and secure extraction rights.[145]

In 2013, a Pentagon report detailed the severity of Chinese based cyber attacks targeting U.S. defense contractors and government agencies. The majority of intrusions aimed at extracting designs for advanced weapon systems. The compromised designs included the Patriot missile system, U.S. Army Terminal High Altitude Area Defense System, the Navy's Aegis system, F/A-18 Hornet, V-22 Osprey, Black Hawk helicopter, the Navy's Littoral Combat Ship, and F-35 Joint Strike Fighter. The article noted that

[144] It is likely that cyber espionage targeting the oil industry and China's territorial claims in the South China Sea reflect two sides of the same strategic coin.

[145] Ellen Nakashima, "Report on 'Operation Shady RAT' Identifies Widespread Cyber-Spying," *The Washington Post,* 3 August 2011, accessed 5 April 2016, https://www.washingtonpost.com/national/national-security/report-identifies-widespread-cyber-spying/2011/07/29/gIQAoTUmqI_story.html.

many of the compromised organizations were wholly unaware their systems were compromised until informed by the Federal Bureau of Investigation. In response, the Pentagon released a report that explicitly "named the Chinese Government and military as the culprit behind intrusions into government and other computer systems." This marked the first instance the United States publicly attributed Chinese cyber espionage to the Chinese government.[146]

Traditional Espionage and Cyber Espionage Compared

Traditional notions of espionage often include sophisticated collectors engaged in a delicate game of spy versus spy where agents construct secret lives in foreign cities while simultaneously guarding and stealing state secrets. All of which requires mastering an esoteric repertoire of field craft techniques in order to meet and recruit sources that have access to the desired information. Although the reality is probably less glamorous, human based espionage requires agents on the ground. This inherently increases the risk of compromise and capture. While agents on the ground are helpful, it does not guarantee access to the desired information. Additionally, the arduous task of recruiting, training, and employing spies means that there will almost always be more intelligence requirements than can be filled, meaning that only the requirements of sufficiently high priority will receive the preponderance of resources. However, the advent of the Internet,

[146] Ellen Nakashima, "Confidential Report Lists US Weapons System Designs Compromised By Chinese Cyberspies," *The Washington Post*, 27 May 2013, accessed 5 April 2016, https://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html; Magnus Hjortdal, "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence," *Journal of Strategic Security* 4, no. 2 (2011): 9.

the digitization of information and the development of cyber-personas have all created a powerful combination enabling cyber espionage.

Cyber espionage allows individuals with no knowledge of traditional espionage to infiltrate and extract massive amounts of information. Whereas in the past collectors would invest weeks and months recruiting sources, now that time can be spent silently conducting reconnaissance on the targeted system probing for security weak spots and searching for the most valuable data to extract. The most likely scenario is that "human and cyber intelligence collection operations have become complementary elements of a broad Chinese economic espionage campaign."[147]

Nonetheless, the barrier to entry for cyber espionage is much lower for a couple reasons. First, as mentioned before, no knowledge of traditional spy craft is necessary which allows collectors to focus exclusively on refining their cyber skills. Second, there is no limit on the types of information that can be collected. For example, in traditional espionage, an agent targeting a defense contractor should have fluent command of the native language and understand the technical aspects of the targeted system. This is far less important in cyber espionage. It is possible to infiltrate government networks, critical infrastructure, businesses, social networking sites, and press organizations. Third, many organizations incorrectly assume that their information is not particularly useful and invest little into cybersecurity, offering attackers a soft target. Fourth, the inability to conclusively attribute cyber intrusions back to a host government creates de facto

[147] Jon R. Lindsay and Tai Ming Cheung, "From Exploitation to Innovation: Acquisition, Absorption, and Application," in *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, ed. Jon R. Lindsay, Tai Ming Cheung, Derek S. Reveron (New York: Oxford University Press, 2015), 56.

plausible deniability. This situation reduces a government's willingness to crackdown on unsanctioned cyber activities as long as it supports national interests. Moreover, a lack of attribution opens the aperture on who is authorized to conduct cyber espionage to include government employees, science and technology centers, and freelance hacktivists. Each of these factors makes cyber espionage increasingly appealing to all governments, but especially those seeking to develop advanced military capabilities, control information flow and achieve greater geopolitical influence.

863 Program and Chinese Modernization

China's interest in network warfare, information dominance and cyber espionage finds its inspiration within formal Chinese science and technology advancement initiatives established throughout the decades since the founding of the PRC. The 863 Program is one such program. Formalized in 1986, Chinese leaders designed the 863 Program to "yoke technological achievements to strategic goals of the state."[148] The overarching goal of the 863 Program was to close the technology gap between China and other developed countries, specifically the United States. In the 1980s, China's minister for the electronics industry, Jiang Zemin, argued that, "IT capabilities constituted the strategic high ground in international competition . . . The discrepancy between China's level and the world's advanced level is so great that we have to do our utmost to catch

[148] Evan A. Feigenbaum, *China's Techno-Warriors: National Security and Strategic Competition from the Nuclear to the Information Age* (Stanford, CA: Stanford University Press, 2003), 163.

up."[149] Ways to close the gap included investing in domestic research, overtly purchasing technology from developed nations, and subversive collection intended to steal technology. Currently, "industrial and cyber espionage activities and other illicit and gray acquisition strategies thus feature prominently in China's efforts to achieve its development goals in priority areas as well as sensitive defense and dual use technologies."[150]

However, the 863 Program was not the only plan implemented to close the gap. By 1992, the "863 Program was one of five pillars that supported China's twenty-first century technology agenda."[151] Even today "there are currently eight such 863 national research centers" tasked to conduct research and development within their specialty. Broadly speaking the national centers are concerned with acquiring relevant technologies within the fields of information technology, automation, biotechnology, new materials, and lasers. "Ultimately, the goal of strategic guidance plans such as 863 is to create an indigenous Chinese capability to innovate and manufacture."[152] Consequently, China "has shown a single-minded determination to acquire the necessary technology and intellectual property rights by whatever possible means."[153] The importance of 863

[149] Nigel Inkster, "China in Cyberspace," in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World,* ed. Derek S. Reveron (Washington, DC: Georgetown University Press, 2012), 192.

[150] Lindsay and Cheung, 74.

[151] Feigenbaum, 163.

[152] Ibid., 201.

[153] Inkster, "China in Cyberspace," 203.

Program and similar initiatives is not to achieve technological development for the sake of scientific discovery, but in direct response to the perception that China remains technologically backwards and ill equipped to compete in the twenty-first century.[154]

The Gulf War

The 1991 U.S.-led coalition against Iraq offers a compelling lens for understanding China's aggressive cyber espionage strategy. For many Americans the stunning victory represented a proverbial rebirth of American exceptionalism and the return of the U.S. military from the post-Vietnam fiscal wilderness. US military planners assessed that Saddam's Iraqi Army, one of the largest in the world, with recent combat experience fighting Iran, would put up a stiff fight. Consequentially, the United States, who had not fought a near competitor since Korea, concentrated significant combat power. As a result, the United States steam rolled Iraqi armor divisions and punished units frantically retreating into Iraqi territory.

The First Gulf War was notable for the speed and ease with which the coalition destroyed Iraq's million-man army. Aerial shock and awe was possible through the employment of a robust electronic warfare and jamming campaign targeting Iraq's Integrated Air Defense System and made more lethal using precision-guided

[154] Reference the Chinese Government's, *The National Medium- and Long-Term Program for Science and Technology Development (2006-2020)*, which includes a number of industries that the government is determined to develop indigenous innovation. Subsequent 863 Programs are best understood as China's periodic *Five Year Plans*.

munitions.[155] Ground based maneuver forces employed advanced communications systems, allowing commanders to maintain high levels of situational awareness. While setting the theater took over six months, once the ground war started, it took only four days for Saddam to agree to the U.S. ceasefire proposal.

The Chinese military witnessed the 1991 Gulf War with equal parts amazement and alarm. In fact, several Chinese military theorists characterize the First Gulf War as an indication of the emergence of a "new era in warfare, a Revolution in Military Affairs (RMA), in which information technology completely revolutionized warfare and changed the way militaries were organized, led, and fought."[156] Additionally, "U.S. military prowess displayed during Operation Desert Storm convinced China's military thinkers of the need to confront a modern adversary on and off the traditional battlefield."[157] One of the preeminent lessons learned by the Chinese is that, "A key component to the West's success was its reliance on a new set of military options focused on information

[155] Carlo Kopp, "Operation Desert Storm The Electronic Battle Parts 1–3," *Australian Aviation* (June, July, August 1993), accessed 8 April 2016, http://www.ausairpower.net/Analysis-ODS-EW.html.

[156] Anthony H. Cordesman and Steven Colley, *Chinese Strategy and Military Modernization in 2015: A Comparative Analysis* (Washington, DC: Center for Strategic and International Studies, October 2015), 129.

[157] Eric C. Anderson and Jeffrey G. Engstrom, "Capabilities of the Chinese People's Liberation Army to Carry Out Military Action in the Event of a Regional Military Conflict" (East Asia Studies Center, Strategic Assessment Center, Advanced Analytics and Linguistics Division, Mission Integration Business Unit, Science Applications International Corporation Tysons Corner, VA, March 2009), accessed 13 May 2016, http://origin.www.uscc.gov/sites/default/files/Research/CapabilitiesoftheChinesePeople'sLiberationArmytoCarryOutMilitaryActionintheEventofaRegionalConflict.pdf, 15.

technologies."[158] This realization implied the importance of obtaining advanced military technology and developing a strategy enabling a technologically weaker force to defeat a stronger more technologically advanced adversary.

Concept of Unrestricted Warfare

The book *Unrestricted Warfare* provides valuable insights for understanding Chinese cyber espionage. Written by two PLA colonels and published in 1999 by the PLA Press, the book offers military leaders an intellectual framework from which to derive a strategy for dealing with future war. Laced with references to the Gulf War this work is part military history and part philosophy; effectively harmonizing Chinese military strategic culture. The authors argue that the Gulf War, "unfolded and concluded for all to see, with its many combatant countries, and glorious results startling the whole world, who could say that a classic war heralding the arrival of warfare in the age of technical integration-globalization."[159] This perspective forms the nucleus of their argument, which is that the Gulf War fundamentally changed the nature of warfare.

However, the concept of unrestricted warfare is not an oblique reference to the Western concept of total war but describes the importance of combining an ever-increasing set of means and ways in pursuit of national objectives. This concept is culturally related to Sun Tzu's description of normal (*cheng*) and extraordinary (*ch'i*)

[158] Timothy L. Thomas, *The Dragon's Quantum Leap: Transforming From a Mechanized to an Informatized Force* (Fort Leavenworth, KS: Foreign Military Studies Office, 2009), 10.

[159] Colonel Qiao Liang and Colonel Wang Xiangsui, *Unrestricted Warfare: Translated From the Original People's Liberation Army Documents* (Brattleboro, VT: Echo Point Books and Media, 1999), 48.

forces but not a direct parallel and seeks to move above the tactical and beyond creative stratagems.[160] The authors argue that this mode of warfare stands in stark contrast to the American way of war, which is called "American-style extravagant warfare" and characterized by a reliance on "high-technology, high investment, high-expenditure and high-payback."[161] This style of warfare depends upon playing by the rules as they were and not as they are. In other words, "the most ideal method of operation for dealing with an enemy who pays no regard to the rules is certainly just being able to break through the rules."[162] This is accomplished by using combination and addition to achieve an "inexhaustible variety of methods of operation."[163] Unrestricted warfare can be understood as "modified combined war that goes beyond limits."[164]

For example, combining and adding military, trans-military, and non-military means provides decision makers with an endless supply of useful combinations that can be adjusted as necessary in pursuit of national objectives. It is also necessary to generate supra-national combinations. "The subtle excellence of application lies in one-mindedness" and "having the myriad methods converge into one." The goal is to

[160] Sun Tzu, *The Art of War,* trans. by Samuel B. Griffith (New York: Oxford University Press, 1963), 91; David Lai, *Learning From the Stones: A Go Approach to Mastering China's Strategic Concept, Shi* (Carlisle Barracks, PA: Strategic Studies Institute, U.S. Army War College Press, May 2004), 1-34.

[161] Liang and Xiangsui, 76. The authors use the word "payback" but western readers should interpret as "pay off."

[162] Liang and Xiangsui, 114.

[163] Ibid., 123.

[164] Ibid., 155.

"assemble and blend together more means to resolve a problem in a range wider than the problem itself." This more often than not requires applying ways and means beyond what the military can provide.[165]

A key objective of *Unrestricted Warfare* is outlining how information technology has changed the battlefield. The authors argue that, "What must be made clear is that the new concept of weapons is in the process of creating weapons that are closely linked to the lives of common people." This refers to the application of everyday technology in the conduct of war. This includes information technology designed to facilitate social interaction and productivity. These "kinder weapons" are the result of technological advancements. The authors contend that "technology is again running ahead of the military thinking" requiring renewed focus on how to fight in the electromagnetic spectrum and network spaces.[166]

One of the most compelling insights provided by the authors is a description of the side-principal. Explaining, "we believe this side-principal relationship exists in a big way in the movement and development of many things, and that in such a relationship the 'side' element, instead of the 'principal' element, often plays the role as the directing element." The relationship between frontline soldiers and the command headquarters reveals this distinction. The soldiers making up the armed force constitute the principal element while the command headquarters is the directing and thus the side element. Employing the side principle means that the most meaningful attacks should be directed

[165] Ibid., 123, 125, 155, 158.

[166] Ibid., 16, 19, 31.

towards the command headquarters, which constitutes the side element. The asymmetrical relationship created by the side element in relation to the principal element makes this concept powerful. Liang and Xiangsui unpack the concept further by referring to LH’s concept of the “indirect strategy.” However, they are careful to emphasize that the side-principal constitutes a “principle” not a “theorem” and should be understood “in terms of lines of thought and essence” not “mechanical application.” The side-principal concept provides a way to think about the most advantageous line of attack but is not prescriptive in nature.[167]

Liang and Xiangsui maintain that the crux of unrestricted warfare is “the concept of exceeding limits which is, first of all, to transcend ideology.” Again, this is not a reference to nuclear strikes or total war but a reminder that “those who are engaged in warfare must break out of the confines of domains if they are to be able to enter a state of freedom in thinking about warfare.” The authors conclude with a list of “essential principles” to conduct unrestricted warfare. The principles are: omnidirectionality, synchrony, limited objectives, unlimited measures, asymmetry, minimal consumption, multidimensional coordination, and adjustment and control of the entire process. The authors do an excellent job explaining the overarching concept and provide useful examples; however, they fail to explain the role of command and control and operational oversight. Arguably, these two areas are responsible for combining and nesting the various means and ensuring adherence to the abovementioned principles.[168]

[167] Liang and Xiangsui, 135, 136, 144, 146-147.

[168] Ibid., 154, 161, 177.

Understanding the logical flow of the arguments within *Unrestricted Warfare* provides readers with a fascinating view into Chinese military thought. While not doctrinally prescriptive, the book received wide acknowledgment throughout the PLA and broader CCP. Of note is the importance of the Gulf War, the role of technology in future war, and the proposal of essential principles.

Integrated Network Electronic Warfare (INEW)

In order to defeat a technologically superior enemy China has adopted a strategy termed INEW. INEW is the strategic output of China's broader transition to the development of "informatized warfare" capabilities.[169] In February of 2014 China established a new organization that is "responsible for developing policies related to computer network operations and Internet security."[170] This new organization is "directed by the chairman of the CCP Central Military Commission (CMC), Xi Jinping, and includes PLA chief of the General Staff."[171] This demonstrates the level of attention and resources China has dedicated to information warfare. Unsurprisingly, Chinese strategists conclude that, "information warfare plays a critical role in modern warfare and that

[169] Bryan Krekel, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation* (prepared for The US-China Economic and Security Review Commission, Northrup Grumman, McLean, VA, 9 October 2009), 6; Timothy Thomas, "Sun Tzu at the Computer: Informationising the 'Art of War'," *CLAWS Journal* (Summer 2009): 164.

[170] Mark Stokes, "The Chinese People's Liberation Army Computer Network Operations Infrastructure," in *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, ed. Jon R. Lindsay, Tai Ming Cheung, Derek S. Reveron (New York: Oxford University Press, 2015), 164.

[171] Ibid.

cyberwarfare . . . is a main form of information warfare."[172] Chinese military leaders argue that, "information operations are described as the most important operational method of modern warfare with electronic and computer network warfare considered the main types of information operations."[173]

INEW flows from an intellectual wellspring that believes information warfare has the potential to "play a decisive role in future conflicts by debilitating information systems critical to military operations and the civilian economy."[174] INEW is unique because it combines electronic warfare and computer network operations.[175] Most Western nations, the United States included, distinguish between the two. However, the PLA hopes to employ this powerful combination by focusing on attacking "an adversary's command, control, communications, computers, intelligence, surveillance, and reconnaissance networks and other essential information systems."[176] The PLA approach focuses on "key point strikes" against an adversary's center of gravity.[177] The purpose is to "affect operations and bring about victory."[178] The PLA expects these attacks to occur simultaneously across every domain (space, air, sea, land, and cyber)

[172] Pollpeter, 138.

[173] Ibid., 141.

[174] Ibid., 151.

[175] Krekel, 7.

[176] Ibid.

[177] Pollpeter, 142.

[178] Ibid.

forcing the adversary to operate under "informatized conditions." Timothy Thomas, a senior analyst at the U.S. Army's Foreign Military Studies Office, notes that, "the foci of Chinese information attacks are enemy command centers, information systems, and information capabilities rather than troop formations as in the past."[179]

INEW operations are "characterized by the combined employment of network warfare tools and electronic warfare weapons against an adversary's information systems in the early phases of a conflict."[180] Consequently, INEW operations form a key component of China's national military strategy, especially during shaping operations within phase zero. The goal of INEW is to "attack only key nodes through which enemy command and control data and logistics information passes and which are most likely to support the campaign's strategic objectives."[181] This capability denotes significant pre-attack reconnaissance, mapping critical infrastructure, and constructing a repertoire of backdoors and footholds within adversary systems. PLA Major Peng Hongqi, in a recent article published in the PLA sponsored *China Military Science* journal, argues that, "the only way the inferior side can compete with a powerful enemy is by taking full advantage of peace-time to energetically elevate its material and technological foundation."[182] This constitutes an area of concern for U.S. defense leaders when understood that Peng advocates that, "an inferior force must conduct information reconnaissance and prepare

[179] Thomas, 170.

[180] Krekel, 10.

[181] Ibid., 15.

[182] Thomas, 168.

confrontational responses as asymmetric checks and balances on an opponent's strategy."[183] INEW capabilities in conjunction with problematic attribution make peacetime reconnaissance not only possible but also highly appealing.

It is clear that China's emphasis on information technology, and specifically cyber espionage, is not a passing phenomenon. It has clear roots in strategic thinking about the ways and means to achieve greater indigenous innovation and the development of advanced military capabilities necessary for success in future warfare. The adoption of INEW and the tremendous level of buy in from key leaders within the CCP, including Xi Jinping, demonstrates the importance China has placed on information warfare. Accordingly, it is expected that China will look for opportunities to further refine and accelerate their capacity to conduct cyber espionage. The remainder of this case study will take a closer look at Chinese cyber espionage and how it is conducted and concludes with an application of LH's indirect approach principles.

PLA-Sponsored Cyber Espionage

Categorically, the majority of Chinese sanctioned cyber espionage are APTs. APTs are defined as, "a cyberattack campaign with specific, targeted objectives, conducted by a coordinated team of specialized experts, combining organization, intelligence, complexity, and patience."[184] Cyber experts characterize APTs by their persistent pursuit of specific information. In China's case, "APT targets include defense technology, foreign government policy regarding Chinese interests, positions of US

[183] Ibid., 167.

[184] Singer and Friedman, 293.

presidential candidates, Chinese dissident activity, and wide range of industries."[185] Additionally, some argue, "All industries related to China's strategic priorities are potential targets of [a] comprehensive cyber espionage campaign."[186]

In 2013, U.S. based cybersecurity firm, Mandiant, a company within FireEye, published a comprehensive report detailing the severity of Chinese sponsored cyber espionage. The report focused on a specific APT referred to as APT1. This moniker correlates to the PLA Unit 61398, which focuses on cyber attacks against English speaking nations and the United States in particular. Unit 61398's physical location is in Shanghai and is task organized under the PLA's General Staff Department, 3rd Department which focuses on signals intelligence and computer network operations.[187]

A successful APT attack generally follows eight steps or phases. These steps include: initial reconnaissance, initial compromise, establish foothold, escalate privileges, internal reconnaissance, move laterally, maintain presence, and complete mission.[188] While these steps are sequential, the APT will conduct iterative attempts to escalate privileges and move laterally through the system. This is done for two reasons. First, APTs typically begin with low-level access insufficient to obtain the targeted information. Second, the ability to move throughout the system and avoid compromise

[185] Lindsay and Cheung, 63.

[186] Mandiant, *APT 1: Exposing One of China's Cyber Espionage Units* (Intelligence Report, Mandiant, Milpitas, CA, 2013), 24, accessed 13 May 2016, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

[187] Ibid., 8; Stokes, 164.

[188] Mandiant, 27.

requires administrator or root access. The mission is complete once all relevant information has been extracted. Mandiant observed that APT1 successfully "maintained access to victim networks for an average of 356 days" with the longest being "1,764 days, or four years and ten months."[189]

The initial reconnaissance phase denotes a host of activities including identifying the target, detailing the information to extract, and learning about the organization, specifically its task organization and network architecture. This phase can take months of disciplined collection.[190] Analyzing email traffic provides insight into how an organization functions. The purpose of this phase is to increase the likelihood of success and ensure efficiency.

The most common technique for gaining initial access is through "spear phishing."[191] Spear phishing refers to emails containing malicious attachments "targeting a specific organization, and seeking unauthorized access to confidential data."[192] Spear phishing is effective because it applies insights gained throughout the initial reconnaissance phase to generate emails that appear genuine and take advantage of the "trust relationship" between colleagues in a professional setting.[193] This includes "using graphically correct logos, relevant subject titles and message bodies, and creating a sense

[189] Ibid., 3.

[190] Krekel, 60.

[191] Mandiant, 28.

[192] TechTarget, "Spear Phishing," accessed 13 April 2016, http://searchsecurity. techtarget.com/definition/spear-phishing.

[193] Krekel, 55.

of urgency."[194] The emails, which are sent throughout the targeted organization include attachments that if opened introduce malware designed to initiate access and enable further exploitation.

Establishing a foothold ensures "control of the target network's systems from outside the network." Typically, an employee's actual access to the targeted information is irrelevant. It only matters that someone within the organization introduces the malware into the system. In fact, "the users targeted first and the data on their computers are often not the actual target of collection."[195] A key task of the malicious attachment is to create a backdoor capable of overcoming a network's firewall.[196] This is most easily accomplished once inside the network. "The malware that these operators employ often tries to communicate with a pre-established command and control server located in a variety of countries."[197] Commercially available backdoors vary in complexity, but the point is to gain some basic ability to issue a "short and rudimentary set of commands."[198] Another key task is to "collect information about the machine's security configuration, settings, and related system information to solidify their presence."[199]

[194] Ibid., 55.

[195] Ibid., 56.

[196] Mandiant, 30.

[197] Krekel, 58.

[198] Mandiant, 32.

[199] Krekel, 57.

Escalating privileges requires obtaining username and passwords "that allow access to more resources within the network."[200] PLA Unit 61398 typically relies on "publicly available tools to dump password hashes from victim systems in order to obtain legitimate user credentials."[201] Password hashes refers to the mathematical representation of a person's actual password. The password hash is stored on the organization's network and is used to validate an individual's username and password at each login. APTs will extract the organization's password hashes and, at their leisure, use various tools to crack the actual password and increase access.[202]

The internal reconnaissance phase focuses on mapping the network and identifying the location of key nodes.[203] This enables the attacker to understand how the network is configured from a cybersecurity perspective and to identify how/where information is stored. In the physical world, this is analogous to obtaining a hologram blueprint of a physical target. The reconnaissance phase is "sufficiently methodical and quiet to permit the compilation of an accurate map of the network over time."[204] This reconnaissance sets conditions for the next phase. "Attackers have also demonstrated an awareness of a targeted organization's information security measures…and appear able to

[200] Mandiant, 34.

[201] Ibid.

[202] Ibid., 35.

[203] Ibid.

[204] Krekel, 61.

alter their operations to avoid detection."[205] By moving through the system carefully, attackers can understand in real time how the organization conducts network security. In the physical world, this is analogous to a special reconnaissance team maintaining eyes on a target in order to understand the strength and routines of the enemy in preparation for follow on exploitation.

Lateral movement through the network is possible after obtaining sets of "legitimate credentials" and understanding the network's layout.[206] In the physical world, this movement is analogous to mapping out a multi storied building by walking through each floor and becoming familiar with the layout and function of each level.

Maintaining presence is accomplished by installing additional backdoors and obtaining multiple legitimate credentials.[207] This is necessary because APTs are built to extract large amounts of information. Maintaining presence gives the attackers time and space to identify the most important information, mitigate emerging security measures and determine the optimal period to extract the information.

The APT completes the mission after consolidating and compressing the targeted files.[208] If the desired files are too large the information will be extracted in chunks. It was observed that, "their [APT 1] reconnaissance of the network enabled them to select

[205] Ibid., 57.

[206] Mandiant, 36.

[207] Ibid., 36.

[208] Ibid., 37.

servers that offered the highest performance and network throughput."[209] In one case, Mandiant observed an "APT1 intruder return to a compromised system once a week for four weeks in a row to steal only the past week's emails."[210] PLA APTs can control multiple servers at a time to expedite the extraction of large amounts of information.[211] Additionally, many commercially available tools enable attackers to quickly sift through available date and refine the type of information extracted.

Over the years PLA sponsored APTs continue to refine their processes. It is noted that, "China's intelligence agencies in respect to foreign collection has evolved from one of great caution and risk aversion to one of greater operational self-confidence commensurate with China's rising status and influence in the world."[212] Evidence of this is seen in not only by what PLA APTs extract but what they leave behind. In one case, "Attackers selected the data for extraction with great care…they did not simply 'take what they could get' and leave, rather, they chose specific files."[213] The attacker also did not spend time opening and searching through all the files extracted, which they could have. Instead they methodically selected only the files of value. This indicates that the attackers had a "shopping list" of information to extract and that the existence of a

[209] Krekel, 63.

[210] Mandiant, 38.

[211] Krekel, 64.

[212] Inkster, "The Chinese Intelligence Agencies: Evolution and Empowerment in Cyberspace," 34.

[213] Krekel, 59.

reliable foothold allowed them to “review the directory contents offline.”[214] This demonstrates that PLA cyber espionage capabilities continue to evolve and that China is not simply interested in a quantitative capability but also one that is qualitative.

LH’s Indirect Approach Principles

The remainder of this chapter analyzes how faithfully, and with what correlation, Chinese cyber espionage applies to LH’s indirect approach principles. The analysis includes strategic and tactical perspectives with emphasis on why China embraces far-reaching cyber espionage and how it is conducted. A detailed explanation of LH’s principles is contained in chapter three.

Adjust ends to means, refers to embracing a strategy of limited aim in order to await a favorable shift in balance. Strategically, this principle speaks directly to China’s historical efforts at modernization and their desire to develop indigenous innovation through the accumulation of internationally obtained science and technology. China acknowledges that the United States is the dominant military and technological power. They cannot achieve the global status they seek until they eclipse the United States. China has the means (technical expertise and national level authority) to develop cyber capabilities. Likewise, cyber espionage facilitates the extraction and importation of valuable technology that China is unable to develop holistically. In this sense, the end is technological parity with the United States and the means is cyber espionage. This principle is also expressed in *Unrestricted Warfare* as “Limited Objectives: objectives

[214] Krekel, 59.

must always be smaller than measures."[215] For these reasons cyber espionage does adhere to this principle.

Keep the object always in mind, highlights that accomplishing the objective is more important than the means employed. It is clear that China embraces a broad cyber espionage campaign that is wedded to their strategic priorities. The international community has repeatedly used the media to accuse China of stealing IP, probing networks, and mapping critical infrastructure. However, China has not stopped cyber espionage operations and has sought to improve its processes. The issues of attribution and acceptable retaliation make it difficult to counter the attacks. Arguably, China understands this well and is steadfastly resolved to achieve their long-term objectives. Additionally, *Unrestricted Warfare* includes two related principles. The first is, "Adjustment and Control of the Entire Process: Any attempt to tie a war to a set of ideas within a predetermined plan is little short of absurdity or naïveté."[216] The second is, "Minimal Consumption: The rational designation of objectives and the rational use of resources." Both of these principles describe the careful consideration and formulation of objectives. For these reasons cyber espionage does adhere to this principle.

Choose the line (or course) of least expectation, is concerned with achieving psychological surprise. Strategically, cyber espionage takes advantage of the misguided perspective among many companies that their IP is both safeguarded and of no value to

[215] Liang and Xiangsui, 179.

[216] Ibid., 185.

attackers.[217] This misconception results in a lack of resources dedicated to cybersecurity, making it easier for attackers to overcome archaic security measures and prevents victims from knowing their property was extracted in the first place. The best example of this is found within the advanced persistent threat cycle, which relies on spear phishing to gain an initial foothold. The targeted recipient is unaware that they received a fraudulent email and more surprised when they discover that the attachment contained malicious code. For these reasons cyber espionage does adhere to this principle.

Exploit the line of least resistance, seeks to achieve physical surprise. Somewhat related to the previous principle, this one emphasizes that any course can be used "so long as it can lead you to any objective which would contribute to your underlying object."[218] Strategically this principle illuminates why pursuing a policy of cyber espionage is effective for the Chinese. Simply put, it provides a low-resistance way to achieve their objectives. It is possible for the Chinese to go a circuitous route to technological innovation because it is the cheapest (financial and political risk) and the most effective. At the tactical level, this principle refers to spear phishing that enables an initial foothold but does not lead the attackers directly to the information they seek. Instead, the attacker must move laterally through the system and elevate their access. For these reasons cyber espionage does adhere to this principle.

[217] Booz Allen Hamilton, *Cyber Theft of Corporate Intellectual Property: The Nature of the Threat* (McLean, VA: Economist Intelligence Unit, Booz Allen Hamilton, 2012), 6; Phoenix Contact, "Hacking the Industrial Network" (A White Paper, Phoenix Contact, Harrisburg, PA, undated).

[218] Liddell Hart, *Strategy*, 335.

Take a line of operation which offers alternative objectives, emphasizes putting the enemy on the "horns of a dilemma" by forcing the enemy to dilute their combat power in an effort to safeguard multiple vulnerable locations. Executed correctly, an enemy's decision making is paralyzed. This principle is the essence of the PLA's INEW concept and articulated in *Unrestricted Warfare* as "Unlimited Measures: The continual enlargement of the range of selection and the methods of use of measures."[219] At the strategic level, cyber espionage forces the victim to choose between a policy commensurate with the level of attacks or one that seeks to minimize intrusions and avoid economic disruption. A resolute stance against China risks jeopardizing productive economic and diplomatic relations, while a hollow policy ensures positive economic ties but does not address endemic cyber intrusions. At this point in time either policy would necessitate significant tradeoffs making it difficult to determine how second and third order effects would destabilize the international system. Evidence of this is seen through the seemingly futile attempts to enact sanctions or enforce the September 2015 U.S.-China public proclamation prohibiting cyber espionage.[220] At the tactical level, businesses and organizations are faced with the options to devote scarce resources towards cybersecurity, turn a blind eye to intrusions, or further restrict internal access to

[219] Liang and Xiangsui, 180.

[220] Ellen Nakashima and Steven Mufson, "U.S., China Vow Not to Engage in Economic Cyberespionage," *The Washington Post*, 25 September 2015, accessed 25 April 2016, https://www.washingtonpost.com/national/us-china-vow-not-to-engage-in-economic-cyberespionage/2015/09/25/90e74b6a-63b9-11e5-8e9e-dce8a2a2a679_story.html.

information, all of which may result in lost efficiency, productivity, and profit. For these reasons cyber espionage does adhere to this principle.

Ensure that both plan and dispositions are flexible—adaptable to circumstances, discusses the importance of promoting a flexibility of mind that allows planners and decision makers to adjust their approach to the actual situation. Chinese programs like the 863 Program are intended to cast a wide net in terms of how science and technology is obtained and introduced into the Chinese system. As mentioned above, cyber espionage constitutes one such method. At the strategic level, cyber espionage is both politically and operational feasible. It is politically feasible due to an inability to achieve conclusive attribution. This hinders defensive cyber efforts and often confines accusations to the court of public opinion. It is operationally feasible because attackers have demonstrated the desire and capacity to strike a broad range of targets in industry and government. This means that attackers have the flexibility to strike soft targets at will and build/obtain the necessary tools to launch attacks against harder targets. The existence of a hard target does not stop cyber espionage and it cannot guarantee impregnable defenses. Additionally, *Unrestricted Warfare* contains the principle of "Omnidirectionality: When observing the battlefield or potential battlefield, designing plan, employing measures, and combining the use of all war resources which can be mobilized, to have a field of vision with no blind spots, a concept unhindered by obstacles, and an orientation with no blind angles."[221] For these reasons cyber espionage does adhere to this principle.

[221] Liang and Xiangsui, 117.

Do not throw your weight into a stroke whilst your opponent is on guard—whilst he is well placed to parry or evade it, advises not to strike in a way that reinforces an enemy's strengths or consolidates his defenses. This is essentially the overarching goal of INEW, which seeks to neutralize command nodes and paralyze decision-making. Likewise, this principle applies to the initial reconnaissance phase of an APT attack. During this phase attackers are able to gain important insights into the company hierarchy and cyber security, which enables the attackers to avoid strengths and attack weaknesses. *Unrestricted Warfare* includes the principle "Asymmetry: Create power for oneself and make the situation develop as you want it to . . . often makes an adversary which uses conventional forces and conventional measures as its main combat strength look like a big elephant charging into a china shop."[222] For these reasons cyber espionage does adhere to this principle.

Do not renew an attack along the same line (or in the same form) after it has once failed, emphasizes that decision makers must not commit additional resources to a failed operation without reassessing the operational variables and employing a different approach. For China sponsored APTs this is not necessarily an overwhelming concern. For example, if a spear phishing operation fails it does not infer that the attackers are defeated or cannot try again. The sheer volume and increasing sophistication of the attacks infers the ability to overcome multiple failures. However, at the strategic level it is precisely because cyber espionage achieves success that it is an integral aspect of

[222] Liang and Xiangsui, 182.

China’s quest to achieve technological parity. For these reasons cyber espionage does not adhere to this principle.

Conclusion

Chinese sponsored cyber espionage does adhere to LH’s principles at the tactical and strategic levels of war. It is clear from analyzing Chinese strategic documents that the PLA is intimately interested in pursuing an indirect approach. Arguably, this method is easily understood by Chinese strategists to be the most effective way to counter a militarily and technologically superior adversary. The PLA published book, *Unrestricted Warfare,* includes eight principles that, while not exact parallels of LH do echo his central concept. Future studies should compare and contrast these principles in order to gain greater insight into PLA strategic thought.

The Chinese Government’s obsession with achieving advanced military capabilities and bridging the technological gap is imprinted in their strategic culture since at least the establishment of the People’s Republic of China in 1949. Evidence of this can be found by analyzing past science and technology programs, especially the 863 Program, and by reading current PLA publications such as open source strategy documents and military science journals. Each of these forums address technological innovation and describe how China intends to use information warfare to defeat “digitized” armies.

The United States faces a serious threat from Chinese cyber espionage. The PLA has invested tremendous resources to build and strengthen this capability. While many experts argue that it is difficult to measure with exactitude the financial impact of cyber espionage it is not difficult to comprehend the danger posed by state sponsored APTs.

Mapping critical infrastructure poses a direct threat to U.S. national security. It is unclear how the Chinese plan to exercise this capability in execution, but insights can be obtained by understanding the role of INEW and the importance of generating meaningful combinations of various means to achieve unrestricted warfare.

CHAPTER 7

CONCLUSIONS AND RECOMMENDATIONS

What can be learned from LH's indirect approach principles? Are they valid? Were they valid in his time? As John Mearsheimer observed, LH was "constantly comparing events, individuals, and situations to find generalizations that would hold across space and time." This unique perspective casts LH's analytical persuasions into equal parts military historian and social scientist. He desperately sought opportunities to apply his knowledge of history to solve Britain's national security problems. His indirect principles are an outgrowth of this desire. However, Mearsheimer and others argue that LH's principles are a circular argument by which all decisive battles throughout history conform to the indirect approach, consequently rendering the framework too elastic to apply objectively.[223]

Nonetheless, LH's indirect approach principles remain valuable for students of military history and as a framework for serious analysis. While it is unlikely that any military theorist will develop a fail proof formula for success it is necessary for military historians to achieve a working knowledge of a broad range of principles and understand their historical roots and relationship to one another. LH's principles provide one such framework for analyzing military history and current operational problems. LH's principles encourage the development of mental flexibility. The application of LH's principles to historical case studies provides the student with a unique lens to analyze decision-making and support the development of a *coup d'oeil*.

[223] Mearsheimer, 10, 87, 89.

Cyberwarfare provides fertile intellectual ground for the application of LH's principles. As noted, Stuxnet and Chinese cyber espionage overwhelmingly adhered to LH's indirect approach principles. Arguably, this is due to the elasticity of the principles. However, it can demonstrate that activities in the cyber domain inherently constitute an indirect approach. This is due to three factors. First, offense currently holds the advantage. This balance places value on the development and employment of offensive capabilities. This is especially true if an attacker has more to gain through offensive action than the defender could achieve by doing the same, which is the case with Chinese cyber espionage targeting U.S. institutions. Second, as Joseph Nye observed, "Strategic studies of the cyber domain are chronologically equivalent to the 1960s but conceptually more equivalent to 1950."[224] In other words, cyber technology/capabilities have greatly outpaced the establishment of strategies, policies, and laws. This reinforces the importance of cyber offense and describes the existence of a man-made cyber wilderness where capabilities in the cyber domain exceed restrictions.

North Korea's cyber attack against Sony, a U.S. company, highlights this phenomenon. Cyber experts quickly attributed the attack to North Korea. but decision makers struggled to classify the attack and disagreed on the proper response. In the end U.S. officials downplayed the significance of the state sponsored attack and categorized it as cybervandalism.[225] Typically, this classification makes it a criminal act, requiring due

[224] Little Limbago, 85.

[225] Steve Holland and Doina Chiacu, "Obama Says Sony Hack Not an Act of War," *Reuters,* 21 December 2014, accessed 28 April 2016, http://www.reuters.com/article/us-sony-cybersecurity-usa-idUSKBN0JX1MH20141222.

process and the input of a prosecution, defendant and a judge. However, President Obama "pledged to respond proportionally to North Korea's alleged cyber assault, in a place, time, and manner our choosing."[226] A few days later, North Korea suffered a nationwide blackout lasting several hours. The United States unconvincingly denied responsibility.[227] Activities in the cyber domain frequently challenge lawmakers to decide the differences between an act of war, terrorism, and a criminal act. This ambiguity yields the advantage to the offense while simultaneously obscuring defensive options.

Third, a defender's inability to achieve high confidence attribution lowers the barriers for offensive action. This will continue to plague cybersecurity professionals who must conduct painstaking cyber forensics to determine an intrusion's severity and source. However, this may not ease efforts to prove conclusively that an attack was state sponsored or part of a nation's national strategy. This is evident in Stuxnet and China's use of advanced persistent threats. Fourth, cyber attacks, by their nature, pursue the path of least resistance. A carefully crafted attack can penetrate the severest of defenses. Stuxnet is an example of this. Similarly, cyber attacks, like Stuxnet, can infiltrate a high priority, yet previously unknown physical locations. This is a profound capability that precision-guided munitions do not have and one that enhances the relevance of offensive

[226] Theohary and Rollins, 1. This CRS report provides an excellent overview on U.S. demarcations regarding cyber attacks as acts of war. The United States takes a firm stance towards using all available means, to include kinetic counter attacks, in response to a cyber attack. However, the key terms and their definitions provide policy makers with considerable latitude; doing little to clear the ambiguity.

[227] Jack Kim, "North Korea Blames U.S. for Internet Outages, Calls Obama 'Monkey'," *Reuters,* 28 December 2014, accessed 4 May 2016, http://www.reuters.com/article/us-northkorea-cybersecurity-idUSKBN0K502920141228.

cyber operations. For these reasons, LH would have embraced cyber activities as a crucial component of any national strategy and certainly one that adhered to his indirect approach.[228]

Stuxnet

LH argued that the “advent of the thermonuclear hydrogen bomb” and the corresponding U.S. policy of massive retaliation resulted in adversaries embracing guerrilla warfare and other “subversive forms of war.” The threat of nuclear war necessitated limited wars that remained below any nation’s nuclear threshold. LH argued that guerrilla warfare was reinvigorated as a mode of warfare uniquely “suited to exploit the nuclear stalemate.” Additionally, there have been many experts, such as former Secretary of Defense Leon Panetta, warning of a cyber Pearl Harbor. In this sense, digital weapons have the destructive potential of a traditional weapons of mass destruction. Ironically, in Stuxnet’s case, a cyberweapon was used to destroy nuclear infrastructure.[229]

Stuxnet validated cyber’s capacity to destroy physical infrastructure. The combined U.S.-Israel cyber attack targeting Iran’s nuclear facilitates showcased this potential. It also highlighted the significant intelligence requirements essential to any offensive cyber operation. In order to be effective Stuxnet’s developers needed exact

[228] Of note, was a failed cyber attack, similar to Stuxnet’s design, targeting North Korea’s nuclear facilities. The attack failed because of North Korea’s unsurprising lack of Internet access. See Andrea Peterson, “A U.S. Cyberattack on North Korea Failed Because North Korea Has Basically No Internet,” *The Washington Post,* 1 June 2015, accessed 4 May 2016, https://www.washingtonpost.com/news/the-switch/wp/2015/06/01/a-u-s-cyberattack-on-north-korea-failed-because-north-korea-has-basically-no-internet/.

[229] Liddell Hart, *Strategy*, 361, 363, 367.

information on the most probable locations of the targeted centrifuges and ways to access them. This required obtaining precise knowledge on the make and model of the centrifuges and all associated components. It was then necessary for developers to test the attack on identical equipment. These rehearsals revealed how the delivery and missile portion would function and identify any gaps in the code. This deliberate process demonstrates the tremendous amount of resources required to mount a successful cyber attack against complex physical infrastructure.[230] Consequently, only large and wealthy states may have the ability to develop such robust capabilities.[231]

Analyzing Stuxnet's use of zero days reinforces this concept. Zero days can be collected through a variety of ways such as purchased on underground markets and by commissioning a large, technically expert workforce tasked to find them. Commercially procured zero day exploits go to the highest bidder, and depending on the cost, may be sold to multiple parties. This reduces the zero days' long-term value. However a talented workforce can identify, catalogue, and consolidate an impressive quantity of exploits, and protect exploits from being sold to adversaries. In either case, zero day exploits require substantial resources, but at the national level, they equal options.

[230] The intense intelligence requirements necessary to develop a potent cyber weapon in conjunction with vague legal precedents are cited as key reasons the United States decided against using cyberattacks against Libya in 2011. See Eric Schmitt and Thom Shanker, "U.S. Debated Cyberwarfare in Attack Plan on Libya," *The New York Times*, 17 October 2011, accessed 10 February 2016, http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html?_r=0.

[231] Erik Gartzke argues, "Cyberwar should be particularly appealing to capable states confronting weaker opponents. Rather than threatening to overturn the existing world order, cyberwar may perpetuate or even increase current military inequality." See Gartzke, 63.

Stuxnet did not deal a decisive blow to Iran's nuclear facilities and certainly not to its nuclear ambitions. However, it can be argued that Stuxnet provided a certain amount of political time and space enabling nuclear negotiations to occur between the United States and Iran. It also showed Iran, that despite their best efforts, the program was vulnerable to attack and that the United States would not permit a nuclear Iran. In addition, a recent news article described a U.S. developed cyber operation called Nitro Zeus that would have been unleashed if Iran failed to agree to the proposed nuclear deal.[232] This may hint at a new utility for cyber operations as bookends to more traditional forms of diplomatic negotiations. In other words, the cyber domain may provide national leaders with the means to conduct coercive action without escalating the confrontation into open hostilities.

China Sponsored Cyber Espionage

Chinese sponsored cyber espionage has grown out of their fervent desire to modernize the military and achieve parity with the United States in information technology. For the Chinese, cyber espionage constitutes ways and means to achieve national objectives. As a way it supports the INEW concept by conducting valuable peacetime reconnaissance in order to map critical infrastructure and identify key nodes within an adversary's system. As a means it provides Chinese leadership with a powerful

[232] Erik Shilling, "From 'Byzantine Hades' to 'Titan Rain', Cyber Attack Code Names are Sci-Fi Poetry," *Atlas Obscura*, 17 February 2016, accessed 5 April 2016, http://www.atlasobscura.com/articles/from-byzantine-hades-to-titan-rain-cyber-attack-code-names-are-scifi-poetry.

capability to extract massive amounts of IP considered vital to their science and technology development strategy and indigenous innovation.

Relentless and pervasive, persistent cyber espionage is less sophisticated than attacks like Stuxnet. An effective cyber espionage campaign does not rely on the meticulous collection and protection of innumerable zero days to achieve success. Instead, cyber espionage relies on detailed pre-attack reconnaissance to inform a smart spear phishing campaign. This does not meant that cyber espionage requires less technical skills, but it does mean that the preponderance of resources can be invested towards building an organization task organized to target specific regions or towards niche aspects of the cyber espionage cycle such as reconnaissance and exploitation.[233] This is why a large and populous country, like China, has a seemingly limitless means to conduct cyber espionage.

There exists debate regarding China's capacity to absorb and integrate all the IP stolen over the past decade. Jon Lindsay and Tai Ming Cheung, both experts in national security affairs, argue that China's aggressive cyber espionage campaign is not a "cheap and effective shortcut for improving industrial innovation" and reject the position that China is "gaining an unfair competitive advantage through cyber espionage."[234] Going further they contend that, "There are real reasons to be skeptical that China's impressive cyber exploitation campaigns can deliver lasting strategic advantage."[235] The authors

[233] Krekel, 56.

[234] Lindsay and Cheung, 54.

[235] Ibid., 52.

point towards two primary reasons. First, the issue of accurately determining the financial cost for victims of cyber espionage remains elusive. The estimations provided by General Keith Alexander, then the head of U.S. Cyber Command, ranged anywhere from $388 billion to $1 trillion globally. While costly, the broad range is problematic because “most damage estimates originate from firms in the business of selling cybersecurity products, so there is reason to be wary of threat inflation.”[236] Second, it is difficult to qualitatively verify that China has utilized the stolen IP. A recent survey completed by company executives on the subject of cyber espionage and IP found that “many executives are optimistic about their companies’ abilities to respond to IP attacks, with 48% of respondents saying that while the theft of IP would cause damage in the short-term, they would be able to recover.”[237] Furthermore, Lindsay and Cheung argue that, “the belief that cyber espionage is a cheap and effective shortcut to improving industrial innovation is harder to substantiate.”[238] However, competing reports recognize that “the breadth of targets and range of potential ‘customers’ of this data suggest the existence of a collection management infrastructure or other oversight to effectively control the range of activities underway, sometimes nearly simultaneously.”[239]

Cybersecurity experts have invested significant resources to investigating, documenting, and publishing reports of Chinese cyber espionage. Yet, there remains a

[236] Lindsay and Cheung, 52

[237] Booz Allen Hamilton, 15.

[238] Lindsay and Cheung, 78.

[239] Krekel, 8.

gap in the literature regarding China's capacity to translate stolen IP into indigenous innovation. This lack of evidence constitutes cold comfort. Historically, China has sought to modernize and develop its information technology capabilities. "In a state that rigorously monitors Internet use, it is highly unlikely that the Chinese Government is unaware of an attack group . . . Therefore the most probable conclusion is that APT1 (Unit 61398) is able to wage such a long-running and extensive cyber espionage campaign because it is acting with the full knowledge and cooperation of the government."[240]

It is likely that the resources devoted to cyber espionage represents the tip of the iceberg, with the greater majority of personnel and attention directed towards developing comprehensive science and technology collection requirements, providing intrusive oversight, and delivering stolen IP to relevant industries and organizations. Cybersecurity firm FireEye acknowledges that, "Although we do not have direct evidence indicating who receives the information APT1 steals or how the recipient processes such a vast volume of data, we do believe that this stolen information can be used to obvious advantage by the PRC and Chinese state-owned enterprises."[241] Future researchers should uncover these tangled connections in order to provide policymakers and industry leaders a more complete picture of how cyber espionage fits into the broader Chinese strategy and how stolen IP is managed internally.

[240] Mandiant, 59.

[241] Ibid., 25.

Cyber as a RMA

Another hotly debated topic deals with cyber as an RMA. Proponents argue that cyber has fundamentally changed warfare, while detractors posit that cyber provides a new set of capabilities similar to the advent of electronic warfare but falls well short of a full-fledged RMA. Williamson Murray and MacGregor Knox contend that military organizations confronting an RMA:

> Must come to grips with fundamental changes in the social, political, and military landscapes. . . . Revolutions in military affairs require the assembly of a complex mix of tactical, organizational, doctrinal, and technological innovations in order to implement a new conceptual approach to warfare or to a specialized sub-branch of warfare.[242]

The concept of "setting the rules of the conflict" is an important component of an RMA. Historically, the side that can take advantage of new technology in a way that alters the rules gains the advantage. This notion deals with anticipating technology's impact on future conflict. This aspect was evident in Prussia's decisive defeat of Austria in 1870, where "Molke succeeded twice in presenting Prussia's adversaries with innovations to which they could not adapt in time to prevent Prussia from setting the rules of the conflict."[243] In this sense, "maneuver must therefore begin before the war started: envelopment was a strategic problem."[244] This concept has direct parallels to cyber.

In *Unrestricted Warfare*, Liang and Xiangsui suggest that advancements in information technology are birthing an emerging RMA. Additionally, "setting the rules"

[242] MacGregor Knox and Williamson Murray, *The Dynamics of Military Revolution 1300-2050* (New York: Cambridge University Press, 2009), 12.

[243] Ibid., 104.

[244] Ibid., 105.

in a future conflict holds the key to maximizing its benefits and “breaking through the rules” as they exist is necessary for survival.[245] Doctrinally, the establishment of combined arms maneuver (CAM) was developed during the interwar period and culminated in the Gulf War. This does not to imply that high intensity CAM has diminished in value since this time. However, CAM fundamentals remain wedded to the example provided during the Gulf War. Advancements in technology are integrated as required to support unified action. This is to say, that while military capabilities have increased the tempo and lethality of modern combat, the fundamentals remain the same.

Arguably, cyber has begun to change how the U.S. we fights, or at least how we think about future wars. However, we military professionals have not yet codified new doctrinal concepts that drastically deviate from conventional combined arms maneuver. This is largely due to the pace of technological advancements. For example, in the time that a technological exploit is realized a reaction and counteraction are developed. This makes it difficult to determine, with precision, the trajectory that technological innovations will take. Technology will have to stabilize to give doctrine a chance to codify and achieve validation. Future research should analyze Russia’s use of cyber in its limited wars against Estonia, Georgia, and their current adventures in Ukraine and Syria. Arguably, this will elicit a solid understanding of how cyber is integrated within CAM, at least as used by a large nation against its weaker contiguous neighbors in the case of Estonia and Georgia.

[245] Liang and Xiangsui, 114.

Conversely, doctrine may require assuming a far less prescriptive role and instead provide a degree of operational latitude permitting deviation in order to take advantage of the fluid nature of technological advancements.[246] The question becomes, at what point do technological advancements cease being referenced only as "lessons learned" or "observed enemy tactics, techniques, and procedures" and begin to be included into doctrine? The answer to this question determines cyber's relevance as an RMA.

Perhaps the key lesson of cyber is its utility as one of a myriad of means that can be employed in a way similar to the method of additive-combinations outlined in *Unrestricted Warfare*. Traditionally, the United States does an excellent job combining the various instruments of national power with an emphasis on the diplomatic, economic, and military.[247] The United States also identifies and develops strategies to achieve peerless dominance across the various domains (space, air, sea, land, and now cyber).

However, U.S. conceptions of instruments of national power and corresponding domains represent a philosophical perspective that views the world in discrete and compartmentalized layers. This promotes stove-piped resource allocation and decision-making. Arguably, this reflects an American culture that instinctively fears monopolization of power and values a system built on separation and checks-and-balances. Conversely, China appears to characterize instruments of national power and

[246] A compelling counterpoint can be found in Libicki's, "Why Cyber War Will Not and Should Not Have Its Grand Strategists," 23-39.

[247] Arguably, the United States understands "Information" as an instrument of power, however, open, pluralistic societies often lack the capacity to issue the clear, unified and concentrated messaging that closed societies have perfected as a matter of national survival.

domains, not as a stack of layers, but a crystalline cube with each component affecting the others simultaneously. This perspective is supported in *Unrestricted Warfare*, which argues that technological advancements have reduced the whole world to a battlefield. This conception may allow for greater synchronization, but it also requires a severely hierarchical and closed system that rewards total obedience and punishes freethinking or unsanctioned innovation.

Can Cyber Achieve Decisive Results?

Currently, it is unlikely that cyber can achieve decisive results on its own. It is far more probable that cyber will continue to increase in relevance within a broader strategic context. However, as seen in Stuxnet and China's cyber espionage, the cyber domain opens up new possibilities to destroy things in the physical world, extract IP and everywhere in between. In this sense, cyber is not simply an additional domain similar to sea or space but unique and separate because it is entirely manmade.

There are three areas where innovations or improvements could alter cyber's offense-defense balance. First is the improved ability to quickly and accurately achieve high confidence attribution. Second is the adoption and enforcement of laws. This is much more difficult than it would appear, and is dependent on multiple factors, not least of which is, determining whether to emphasize information security or network security. China and other closed authoritarian systems prefer the former, while Western nations, which emphasize freedom of information, prefer the latter. The development of laws will depend first on improvements in attribution. Third is the expanding development of the cyber-persona.[248] This is a key variable that continues to evolve through the improvement and development of devices and applications linking people together in cyberspace. While older Americans distinctly recall a time without computers or the Internet, young people are growing up in a hyper-connected environment that places a real or imagined requirement to conduct ceaseless interaction in cyberspace.[249] This includes commenting, posting pictures, downloading upgrades, or purchasing the latest application. In many ways, activities in the physical world plays a supporting role to an online existence. Arguably, at some point a certain degree of governmental interference will be necessary to develop and enforce laws protecting people's cyber personas.

For the near future, offense will continue to hold the advantage. This reality induces states to develop robust cyber capabilities. For smaller nations and non-state actors this requires purchasing commercial exploits or hiring a third party to conduct cyber operations. For large nations like the United States, Russia, and China, this means creating technically expert organizations capable of mounting sophisticated offensive operations. Arguably, it is necessary to develop offensive skills in order to identify and develop a corresponding defensive measure. It is also necessary for nations to conceal the true extent of their capabilities lest they sacrifice a potential advantage. Consequently, we

[248] An interesting discussion on this topic can be found in Kelly Wallace, "Half of Teens Think They're Addicted to Their Smartphones," *CNN*, 3 May 2016, accessed 4 May 2016, http://www.cnn.com/2016/05/03/health/teens-cell-phone-addiction-parents/; for a perspective on the development of legal rights for those affected by online abuse see Danielle Keats Citron, *Hate Crimes in Cyberspace* (Cambridge, MA: Harvard University Press, 2014).

[249] This includes the widespread belief among employees that sending work related emails late at night and throughout the weekend indicates professionalism, a strong work ethic and loyalty to the organization.

are witnessing the initial stages of a cyber security dilemma, with all sides conducting widespread cyber reconnaissance and testing one another’s reactions; probing for weaknesses in infrastructure, laws and national will.

GLOSSARY

Advanced Persistent Threat (APT). A cyber attack campaign with specific, targeted objectives, conducted by a coordinated team of specialized experts, combining organization, intelligence, complexity, and patience.[250]

Air-Gap. To physically isolate a computer or network from other unsecure networks, including the public Internet, to prevent network-enabled attacks.[251]

Anonymous. A decentralized but coordinated collection of users from various Internet forums, who gather to conduct organized attacks, protests, and other actions using cyber means. The most noted of the hacktivist groups, its motives range from political protest to vigilantism to sheer amusement.[252]

Botnet. A collection of computers which have been taken over by a malicious attacker (after an intrusion) who controls their collective actions with another set of computers, called “botnet herders” or “command and control servers.” Botnets can be rented out to raise money for the attacker or can be used to send spam, engage in fraud, or conduct DDoS attacks.[253]

Certificate Authority (CA). A trusted organization that produces signed digital “certificates” that explicitly tie an entity to a public key. This allows asymmetric cryptography users to trust that they are communicating with the right party.[254]

Computer Emergency Response Team (CERT). Organizations located around the world that serve as hubs of cybersecurity technical expertise, collaboration, and security information dissemination. Many governments have their own national computer emergency response teams, as do an increasing number of industrial sectors and large organizations.[255]

Counterespionage. That aspect of counterintelligence designed to detect, destroy, neutralize, exploit, or prevent espionage activities through identification,

[250] Singer and Friedman, 293.

[251] Ibid.

[252] Ibid.

[253] Ibid.

[254] Ibid., 294.

[255] Ibid.

penetration, manipulation, deception, and repression of individuals, groups, or organizations conducting or suspected of conducting espionage activities.[256]

Computer Network Attack. Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.[257]

Computer Network Exploitation. Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks.[258]

Critical Capability. A means that is considered a crucial enabler for a center of gravity to function as such and is essential to the accomplishment of the specified or assumed objective(s).[259]

Critical Infrastructure. The underlying components of the economy that run our modern-day civilization, ranging from power and water, to banking, healthcare, and transportation.[260]

Critical Vulnerability. An aspect of a critical requirement which is deficient or vulnerable to direct or indirect attack that will create decisive or significant effects.[261]

Cyberactivists. Individuals who perform cyber attacks for pleasure, philosophical, political, or nonmonetary reasons. See hacktivist.[262]

Cyber Attack. Using a computer or network to maliciously affect other computers and networks. Attacks require vulnerability and exploit, combined to access to the target.[263]

[256] JCS, JP 1-02, 52.

[257] Ibid., 73.

[258] Ibid.

[259] Joint Chiefs of Staff (JCS), Joint Publication (JP) 5-0, *Joint Operation Planning* (Washington, DC: Government Printing Office, 11 August 2011), GL-8.

[260] Singer and Friedman, 294.

[261] JCS, JP 5-0, GL-8.

[262] Theohary and Rollins, 3.

[263] Healy, 280.

Cyber Conflict. When nations and non-state groups use offensive and defensive cyber capabilities to attack, defend, and spy on each other, typically for political or other national security purposes. Generally does not include cyber crime, but inclusive of cyber war.[264]

Cyber Crime. A criminal act that is mediated through cyberspace, in which computers or networks play an instrumental role, such as DDoS, intrusions or worms.[265]

Cyberspace. A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.[266]

Cyberspace Superiority. The degree of dominance in cyberspace by one force that permits the secure, reliable conduct of operations by that force, and its related land, air, maritime, and space forces at a given time and place without prohibitive interference by an adversary.[267]

Cyber Terrorism. As defined by the Federal Bureau of Investigation, a "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents."[268]

Cyberwar. Actions by a nation-state to damage or disrupt another nation's computers or networks, which are heavily damaging and destructive—similar to the effects achieved with traditional military force—and so are considered to be an armed attack.[269]

Cyberwarriors. Agents or quasi agents of nation-states who develop capabilities and undertake cyber attacks in support of a country's strategic objectives.[270]

[264] Healy, 280.

[265] Ibid.

[266] Joint Chiefs of Staff (JCS), Joint Publication (JP) 3-12 (R), *Cyberspace Operations* (Washington, DC: Government Printing Office, 5 February 2013), GL-4.

[267] Ibid.

[268] Singer and Freidman, 294.

[269] Healy, 281.

[270] Theohary and Rollins, 3.

Defensive Cyberspace Operations. Passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems.[271]

Department of Defense Information Networks. The globally interconnected, end-to-end set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, including owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems.[272]

Distributed Denial of Service (DDoS). An attack that seeks to inundate a targeted system's functions or connections to the Internet. Attackers distribute the overwhelming traffic across multiple sources, often using botnets of thousands or even millions of machines.[273]

Espionage. The act of obtaining, delivering, transmitting, communicating, or receiving information about the national defense with an intent, or reason to believe, that the information may be used to the injury of the United States or to the advantage of any foreign nation. Espionage is a violation of 18 United States Code 792-798 and Article 106, Uniform Code of Military Justice. See also counterintelligence.[274] Ref Counterespionage.

Espionage Against the United States. Overt, covert, or clandestine activity designed to obtain information relating to the national defense with intent or reason to believe that it will be used to the injury of the United States or to the advantage of a foreign nation. For espionage crimes see Chapter 37 of Title 18, United States Code.[275]

Firewall. A filter that rejects data traffic from entering a specific network or machine following specific rules.[276]

[271] JCS, JP 3-12(R), II-2.

[272] Ibid., II-3.

[273] Singer and Friedman, 295.

[274] JCS, JP 1-02 (June 2015), 80.

[275] Ibid., 128.

[276] Singer and Friedman, 295.

Hacktivists. Hacker-activists who conduct their activities on behalf of an ideology. See Anonymous.[277]

Honeypot (or Honeynet). Tactic used by security researchers in which computers, networks, or virtual machines are intentionally exposed to attacks. By observing how different types of malware behave, researchers can identify new types of attacks and devise defenses.[278]

Information Assurance. Actions that protect and defend information systems by ensuring availability, integrity, authentication, confidentiality, and nonrepudiation.[279]

Internet of Things. Superimposing an information environment on top of the real world. As more objects have digital sensors and unique identifiers, the communication and processing powers of cyberspace can be embedded in the real world.[280]

Malware. Malicious or malevolent software, including viruses, worms, and Trojans, that is preprogrammed to attack, disrupt, and/or compromise other computers and networks.[281]

Offensive Cyberspace Operations. Cyberspace operations intended to project power by the application of force in or through cyberspace.[282]

Spear Phishing. E-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data. Spear phishing attempts are not typically initiated by “random hackers” but are more likely to be conducted by perpetrators out for financial gain, trade secrets or military information.[283]

Supervisory Control and Data Acquisition (SCADA). A type of industrial control system, particularly used to monitor and manage interconnected sensors and control large facilities.[284]

[277] Healy, 282.

[278] Singer and Friedman, 295.

[279] JCS, JP 3-12(R), GL-4.

[280] Singer and Friedman, 296.

[281] Ibid., 297.

[282] JCS, JP 3-12(R), GL-4.

[283] TechTarget.

[284] Singer and Friedman, 298.

Shortfall. The lack of forces, equipment, personnel, material, or capability, reflected as the difference between the resources identified as a plan requirement and those apportioned to a combatant commander for planning that would adversely affect the command's ability to accomplish its mission.[285]

Trojan. A type of malware disguised or attached to legitimate or innocuous-seeming software, but that instead carries a malicious payload, most often opening a backdoor to authorized users.[286]

Unit 61398. Also known as the "Comment Crew" and "Shanghai Group," a key unit in the Chinese military tasked with gathering political, economic, and military-related intelligence on the United States through cyber means.[287]

Virus. A malware program that can replicate itself and spread from computer to computer.[288]

Worm. A type of malware that spreads automatically over a network, installing and replicating itself. The network traffic from rapid replication and spread can cripple networks even when the malware does not have malicious payload.[289]

Zero Day. An attack that exploits a previously unknown vulnerability; taken from the notion that the attacks take place on the zeroth day of the awareness. Knowledge about zero day exploits are valuable to both defenders and attackers.[290]

[285] JCS, JP 5-0, GL-15.

[286] Singer and Friedman, 299.

[287] Ibid.

[288] Ibid.

[289] Ibid.

[290] Ibid.

BIBLIOGRAPHY

Books

Blane, John V. *Cyberwarfare: Terror at a Click*. New York: Novinka Books, 2001.

Bond, Brian. *Liddell Hart: A Study of His Military Thought*. Aldershot, VT: Gregg Revivals, 1991.

Bond, Brian, and Martin Alexander. "Liddell Hart and De Gaulle: The Doctrines of Limited Liability and Mobile Defense." In *Makers of Modern Strategy from Machiavelli to the Nuclear Age*, edited by Peter Paret, 598-623. Princeton, NJ: Princeton University Press, 1986.

Carr, Jeffrey. *Inside Cyber Warfare: Mapping the Cyber Underworld*. Cambridge, MA: O'Reilly, 2010.

Cisco Networking Academy. *IT Essentials: PC Hardware and Software Companion Guide,* 5th ed. Indianapolis, IN: Cisco Press, 2014.

Citron, Danielle Keats. *Hate Crimes in Cyberspace*. Cambridge, MA: Harvard University Press, 2014.

Clark, Robert A., and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to do About It*. New York: HarperCollins, 2010.

Corbett, Julian. *Some Principles of Maritime Strategy*. Annapolis, MD: Naval Institute Press, 1988.

Demchak, Chris. "Cybered Conflict, Cyber Power, and Security Resilience as Strategy." In *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, edited by Derek S. Reveron, 121-136. Washington, DC: Georgetown University Press, 2012.

Englemann, Bettina, and Paula Cordaro. *Cyber Commander's Handbook: The Weaponry and Strategies of Digital Conflict*. Cannonsburg, PA: PA Technolytics, 2009.

Feigenbaum, Evan A. *China's Techno-Warriors: National Security and Strategic Competition from the Nuclear to the Information Age*. Stanford, CA: Stanford University Press, 2003.

Gray, Colin. *Making Strategic Sense of Cyber Power: Why the Sky is Not Falling*. Carlisle Barracks, PA: Strategic Studies Institute, U.S. Army War College Press, April 2013.

Healy, Jason, ed. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Arlington, VA: Cyber Conflict Studies Association, 2013.

Inkster, Nigel. “China in Cyberspace.” In *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World,* edited by Derek S. Reveron, 191-206. Washington, DC: Georgetown University Press, 2012.

———. “The Chinese Intelligence Agencies: Evolution and Empowerment in Cyberspace.” In *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain,* edited by Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron, 29-50. New York: Oxford University Press, 2015.

Kalic, Sean. *US Presidents and the Militarization of Space, 1946-1947.* College Station: Texas A&M Press, 2012.

Knox, MacGregor, and Williamson Murray. *The Dynamics of Military Revolution 1300-2050.* New York: Cambridge University Press, 2009.

Kyle, James H. *The Guts to Try: The Untold Story of the Iran Hostage Rescue Mission by the On-Scene Desert Commander*. New York: Orion Books, 1990.

Lai, David. *Learning From the Stones: A Go Approach to Mastering China’s Strategic Concept, Shi*. Carlisle Barracks, PA: Strategic Studies Institute, U.S. Army War College Press, May 2004.

Lewis, Ted G. *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation.* 2nd ed. Hoboken, NJ: Wiley and Sons, 2015.

Liang, Qiao, and Wang Xiangsui. *Unrestricted Warfare: Translated From the Original People’s Liberation Army Documents.* Brattleboro, VT: Echo Point Books and Media, 1999.

Libicki, Martin. *Conquest in Cyberspace: National Security and Information Warfare.* New York: Cambridge University Press, 2007.

Liddell Hart, B. H. *The Decisive Wars of History: A Study in Strategy*. London: Bell, 1929.

———. *Strategy.* 2nd rev. ed. New York: Meridian, 1991.

Lindsay, Jon R., and Tai Ming Cheung. “From Exploitation to Innovation: Acquisition, Absorption, and Application.” In *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain,* edited by Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron, 51-86. New York: Oxford University Press, 2015.

Marquis, Susan L. *Unconventional Warfare: Rebuilding U.S. Special Operations Forces*. Washington, DC: Brookings Institution Press, 1997.

Mearsheimer, John J. *Liddell Hart and the Weight of History.* Ithaca, NY: Cornell University Press, 1988.

Pollpeter, Kevin. “Chinese Writings on Cyberwarfare and Coercion.” In *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain,* edited by Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron, 138-162. New York: Oxford University Press, 2015.

Singer, Peter Warren, and Allan Friedman. *Cyberspace and Cyberwar: What Everyone Needs to Know*. New York: Oxford University Press, 2014.

Stokes, Mark. “The Chinese People’s Liberation Army Computer Network Operations Infrastructure.” In *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, edited by Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron, 163-187. New York: Oxford University Press, 2015.

Sun Tzu. *The Art of War*. Translated by Samuel B. Griffith. New York: Oxford University Press, 1963.

Thomas, Timothy L. *The Dragon’s Quantum Leap: Transforming From a Mechanized to an Informatized Force.* Fort Leavenworth, KS: Foreign Military Studies Office, 2009.

Zetter, Kim. *Countdown to Zero Day: Stuxnet and the Launch of the World’s First Digital Weapon*. New York: Crown Publishers, 2014.

Government Documents

Joint Chiefs of Staff. Joint Publication 1-02, *Department of Defense Military and Associated Terms.* Washington, DC: Government Printing Office, 8 November 2010, as amended through 15 June 2015.

———. Joint Publication 3-12 (R), *Cyberspace Operations.* Washington, DC: Government Printing Office, 5 February 2013.

———. Joint Publication 5-0, *Joint Operation Planning.* Washington, DC: Government Printing Office, 11 August 2011.

Secretary of Defense. *The Department of Defense Cyber Strategy*. Washington, DC: Department of Defense, April 2015.

U.S. Congress. House. *China’s Approach to Cyber Operations: Implications for the United States*. Larry M. Wortzel Testimony Before the Committee on Foreign Affairs, Washington, DC, 10 March 2010.

———. Senate. *Statement of General Keith B. Alexander Commander United States Cyber Command Before the Senate Committee on Armed Services*. Washington, DC, 27 February 2014.

Online Sources

BBC News. "Iranian Nuclear Scientist Killed in Motorbike Attack." *BBC*, 29 November 2010. Accessed 12 February 2016. http://www.bbc.com/news/world-middle-east-11860928.

Brooks, Chris. "Victims of June OPM Hack Still Haven't Been Notified." *Threat Post,* 2 September 2015. Accessed 7 September 2015. https://threatpost.com/victims-of-june-opm-hack-still-havent-been-notified/114512/.

Holland, Steve, and Doina Chiacu. "Obama Says Sony Hack Not an Act of War." *Reuters*, 21 December 2014. Accessed 28 April 2016. http://www.reuters.com/article/us-sony-cybersecurity-usa-idUSKBN0JX1MH20141222.

Internet Live Stats. "China Internet Users." Accessed 7 May 2016. http://www.internetlivestats.com/internet-users/china/.

Iran Watch. "A History of Iran's Nuclear Program." 1 March 2012. Accessed 8 January 2016. http://www.iranwatch.org/our-publications/weapon-program-background-report/history-irans-nuclear-program.

———. "Iran Nuclear Milestones: 1967-2013." 1 June 2013. Accessed 8 January 2016. http://www.iranwatch.org/our-publications/weapon-program-background-report/iran-nuclear-milestones-1967-2013.

Kim, Jack. "North Korea Blames U.S. for Internet Outages, Calls Obama 'Monkey'." *Reuters,* 28 December 2014. Accessed 4 May 2016. http://www.reuters.com/article/us-northkorea-cybersecurity-idUSKBN0K502920141228.

Krebs, Brian. "OPM (mis)Spends $133M on Credit Monitoring," Krebs on Security. September 2015. Accessed 7 September 2015. http://krebsonsecurity.com/2015/09/opm-misspends-133m-on-credit-monitoring/.

McEvers, Kelly. "Rules for Cyberwarfare Still Unclear, Even as US Engages in It." *NPR*, 20 April 2016. Accessed 27 April 2016. http://www.npr.org/templates/transcript/transcript.php?storyID=475005923.

TechTarget. "Spear Phishing" Accessed 13 April 2016. http://searchsecurity.techtarget.com/definition/spear-phishing.

Timmerman, Ken. "Computer Worm Wreaking Havoc on Iran's Nuclear Capabilities." Newsmax, 27 April 2011. Accessed 9 February 2016. http://www.newsmax.com/PrintTemplate.aspx/?nodeid=394327.

United Nations Office for Disarmament Affairs. "Treaty on the Non-Proliferation of Nuclear Weapons." United Nations. Accessed 13 May 2016. http://disarmament.un.org/treaties/t/npt/text.

Wallace, Kelly. "Half of Teens Think They're Addicted to Their Smartphones." *CNN*, 3 May 2016. Accessed 4 May 2016. http://www.cnn.com/2016/05/03/health/teens-cell-phone-addiction-parents/.

Zorabedian, John. "Should the US hit China with Sanctions over Cyber-Espionage?" Naked Security, 3 September 2015. Accessed 7 September 2015. https://nakedsecurity.sophos.com/2015/09/03/should-the-us-hit-china-with-sanctions-over-cyberespionage/?utm_source=Naked%2520Security%2520-%2520Feed&utm_medium=feed&utm_content=rss2&utm_campaign=Feed&utm_source=Naked+Security+-+Sophos+List&utm_campaign=77926f634f naked%252Bsecurity&utm_medium=email&utm_term=0_31623bb782-77926f634f-454898153.

Periodicals

Bonner, Lincoln E. "Cyber Power in the 21st Century Joint Warfare." *Joint Forces Quarterly* (3rd Quarter 2014): 102-109.

Broad, William, John Markoff, and David E. Sanger. "Israeli Test on Worm Called Crucial in Iran Nuclear Delay." *The New York Times*, 15 January 2011. Accessed 11 February 2016. http://www.nytimes.com/2011/01/16/world/middleast/16stuxnet.html?_r=1.

Bumiller, Elisabeth, and Thom Shanker. "Panetta Warns of Dire Threat of Cyberattack on U.S." *The New York Times*, 11 October 2012. Accessed 9 December 2015. http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?_r=0.

Clayton, Mark. "Exclusive: New Thesis on How Stuxnet Infiltrated Iran Nuclear Facility." *The Christian Science Monitor*, 25 February 2014. Accessed 6 September 2015. http://www.csmonitor.com/World/Security-Watch/2014/0225/Exclusive-New-thesis-on-how-Stuxnet-infiltrated-Iran-nuclear-facility.

Dehgan, Saeed Kamali, and Julian Borger. "Iranian Nuclear Chemist Killed By Motorbike Assassins." *The Guardian*, 11 January 2012. Accessed 22 February 2016. http://www.theguardian.com/world/2012/jan/11/iran-nuclear-chemist-killed.

Demchak, Chris C., and Peter Dombrowski. "Rise of a Cybered Westphalian Age." *Strategic Studies Quarterly* (Spring 2011): 32-61.

Follath, Erich, and Holger Stark. “The Birth of a Bomb: A History of Iran’s Nuclear Ambitions.” *Spiegel Online,* 17 June 2010. Accessed 2 February 2016. http://www.spiegel.de/international/world/the-birth-of-a-bomb-a-history-of-iran-s-nuclear-ambitions-a-701109.html.

———. “The Story of ‘Operation Orchard’: How Israel Destroyed Syria’s Al Kibar Nuclear Reactor.” *Speigel Online,* 2 November 2009. Accessed 9 February 2016. http://www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663.html.

Gartzke, Erik. “The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth.” *International Security* 38, no. 2 (Fall 2013): 41-73.

Gorman, Siobhan. “Electricity Grid in US Penetrated By Spies.” *The Wall Street Journal,* 8 April 2009. Accessed 5 April 2016. http://www.wsj.com/articles/SB123914805204099085.

Graham, Bradley. “Hackers Attack Via Chinese Web Sites.” *The Washington Post*, 25 August 2005. Accessed 5 April 2016. http://www.washingtonpost.com/wp-dyn/content/article/2005/08/24/AR2005082402318.html.

Henderson, Scott. “Beijing’s Rising Hacker Stars…How Does Mother China React?” *IO Sphere* (Fall 2008): 25-30.

Hjortdal, Magnus. “China’s Use of Cyber Warfare: Espionage Meets Strategic Deterrence.” *Journal of Strategic Security* 4, no. 2 (2011): 1-24.

Hongqi, Major Peng. “A Brief Discussion of Using the Weak to Defeat the Strong Under Informatized Conditions.” *China Military Science* 1 (2008). Trans. by Open Source Enterprise. Accessed 13 May 2016. https://www.opensource.gov/portal/server.pt/gateway/PTARGS_0_0_200_203_121123_43/content/Display/CPP20080624563002#index=2&searchKey=22611269&rpp=10.

Kaiser, Robert Kaiser. “The Birth of Cyberwar.” *Political Geography* 46 (2015): 11-20.

Kopp, Carolo. “Operation Desert Storm The Electronic Battle Parts 1 – 3.” *Australian Aviation* (June, July, August 1993). Accessed 8 April 2016. http://www.ausairpower.net/Analysis-ODS-EW.html.

Lake, Eli. “Operation Sabotage: Our Secret War Against Iran.” *New Republic,* 13 July 2010. Accessed 22 February 2016. https://newrepublic.com/article/75952/operation-sabotage.

Lee, Melanie. “China’s Nearly 700 Million Internet Users Are Hot for Online Finance.” *Forbes,* 25 January 2016. Accessed 7 May 2016. http://www.forbes.com/sites/melanieleest/2016/01/25/chinas-nearly-700-million-internet-users-are-hot-for-online-finance/#5418bad81391.

Libicki, Martin C. “Why Cyber War Will Not and Should Not Have Its Grand Strategists.” *Strategic Studies Quarterly* (Spring 2014): 23-39.

Liff, Adam P. “Cyberwar: A New ‘Absolute Weapon’? The Proliferation of Cyberwarfare Capabilities and Interstate War.” *The Journal of Strategic Studies* 35, no. 3 (June 2012): 401-428.

Little Limbago, Andrea. “One Size Does Not Fit All: The Multifaceted Nature of Cyber Statecraft.” *Joint Force Quarterly* 78 (3rd Quarter 2015): 84-90.

Lu, Quan Hai T. “Cyber Attacks: The New WMD Challenge to the Interagency.” *Interagency Journal* 6, no. 2 (Spring 2015): 48-57.

Maillard, Laurent. “Iran Denies Nuclear Plant Computer Hit By Worm.” *The Sydney Morning Herald*, 27 September 2010. Accessed 9 February 2016. http://www.smh.com.au/action/printArticle?id=1949566.

Markoff, John. “Cyber Attack on US Nuclear Arms Lab Linked to China.” *The New York Times*, 9 November 2007. Accessed 5 April 2016. http://www.nytimes.com/2007/12/09/world/americas/09iht-hack.1.8653712.html?_r=0.

Mullins, Barry E. “Developing Cyber Warriors From Computer Engineers et al.” *Computers in Education Journal* (2012): 26- 35. Accessed 12 August 2016. https://www.asee.org/public/conferences/8/papers/3146/view.

Nakashima, Ellen. “Chinese Breach Data of 4 Million Federal Workers.” *Washington Post*, 4 June 2015. Accessed 7 September 2015. https://www.washingtonpost.com/world/national-security/chinese-hackers-breach-federal-governments-personnel-office/2015/06/04/889c0e52-0af7-11e5-95fd-d580f1c5d44e_story.html.

———. “Confidential Report Lists US Weapons System Designs Compromised By Chinese Cyberspies.” *The Washington Post*, 27 May 2013. Accessed 5 April 2016. https://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html.

———. “Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say.” *Washington Post*, 9 July 2015. Accessed 7 September 2015. http://www.washingtonpost.com/blogs/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/.

———. “Report on ‘Operation Shady RAT’ Identifies Widespread Cyber-Spying.” *The Washington Post*, 3 August 2011. Accessed 5 April 2016. https://www.washingtonpost.com/national/national-security/report-identifies-widespread-cyber-spying/2011/07/29/gIQAoTUmqI_story.html.

———. “US Publicly Calls on China to Stop Commercial Cyber-Espionage, Theft of Trade Secrets.” *The Washington Post,* 11 March 2013. Accessed 7 September 2015. https://www.washingtonpost.com/world/national-security/us-publicly-calls-on-china-to-stop-commercial-cyber-espionage-theft-of-trade-secrets/2013/03/11/28b21d12-8a82-11e2-a051-6810d606108d_story.html.

Nakashima, Ellen, and Andrea Peterson. “Report: Cybercrime and Espionage Costs $445 Billion Annually.” *The Washington Post,* 9 June 2014. Accessed 7 October 2015. https://www.washingtonpost.com/world/national-security/report-cybercrime-and-espionage-costs-445-billion-annually/2014/06/08/8995291c-ecce-11e3-9f5c-9075d5508f0a_story.html.

Nakashima, Ellen, and Joby Warrick. “Stuxnet Was Work of US and Israeli Experts, Officials Say.” *The Washington Post*, 2 June 2012. Accessed 27 April 2016. https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html.

Nakashima, Ellen, and Steven Mufson. “U.S., China Vow Not to Engage in Economic Cyberespionage.” *The Washington Post,* 25 September 2015. Accessed 25 April 2016. https://www.washingtonpost.com/national/us-china-vow-not-to-engage-in-economic-cyberespionage/2015/09/25/90e74b6a-63b9-11e5-8e9e-dce8a2a2a679_story.html.

Norton-Taylor, Richard. “Titan Rain–How Chinese Hackers Targeted Whitehall.” *The Guardian,* 4 September 2007. Accessed 5 April 2016. https://www.theguardian.com/technology/2007/sep/04/news.internet.

Peterson, Andrea. “A U.S. Cyberattack on North Korea Failed Because North Korea Has Basically No Internet.” *The Washington Post,* 1 June 2015. Accessed 4 May 2016. https://www.washingtonpost.com/news/the-switch/wp/2015/06/01/a-u-s-cyberattack-on-north-korea-failed-because-north-korea-has-basically-no-internet/.

Pu, Peng. “PLA Unveils Nation’s First Cyber Center.” *Global Times,* 22 July 2010. Accessed 30 March 2016. http:www.globaltimes.cn/contents/554647.shtml.

Quick, Christopher R. “Cyberspace as a Weapon System.” *Landpower Essay* no. 14-1 (March 2014): 1-8.

Raiu Costin, G., and Alex Gostev. “A Tale of Stolen Certificates.” *Secureview* (2nd Quarter 2011): 6-10.

Sanger, David E. “US Rejected Aid for Israeli Raid on Iranian Nuclear Site.” *The New York Times,* 10 January 2009. Accessed 26 April 2016. http://www.nytimes.com/2009/01/11/washington/11iran.html?_r=0.

Schmitt, Eric, and Thom Shanker. “U.S. Debated Cyberwarfare in Attack Plan on Libya.” *The New York Times,* 17 October 2011. Accessed 10 February 2016. http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html?_r=0.

Shakarian, Paulo. “Stuxnet: Cyberwar Revolution in Military Affairs.” *Small Wars Journal* (15 April 2011): 1-10.

Shilling, Erik. “From ‘Byzantine Hades’ to ‘Titan Rain’, Cyber Attack Code Names are Sci-Fi Poetry.” *Atlas Obscura,* 17 February 2016. Accessed 5 April 2016. http://www.atlasobscura.com/articles/from-byzantine-hades-to-titan-rain-cyber-attack-code-names-are-scifi-poetry.

Talbot, David. “Cyber-Espionage Nightmare.” *MIT Technology Review,* 15 June 2015. Accessed 25 September 2015. http://www.technologyreview.com/featuredstory/538201/cyber-espionage-nightmare//

Thomas, Timothy. “The Chinese Military’s Strategic Mind-Set.” *Military Review* (November-December 2007): 46-55.

———. “Sun Tzu at the Computer: Informationising the ‘Art of War’.” *CLAWS Journal* (Summer 2009): 164-182.

Vaez, Ali. “Waiting for Bushehr: The Long Wait for Iran’s First Nuclear Power Plant is Finally Over. It’s Now Online, But is it Ready?” *Foreign Policy,* 12 September 2011. Accessed 22 February 2016. http://foreignpolicy.com/2011/09/12/waiting-for-bushehr/.

Warrick, Joby. “U.S. Is Said to Expand Covert Operations In Iran: Plan Allows Up to $400 Million for Activities Aimed at Destabilizing Government.” *The Washington Post,* 30 June 2008. Accessed 22 February 2016. http://www.washingtonpost.com/wp-dyn/content/article/2008/06/29/AR2008062901881.html.

Young, William, and Robert Worth. “Bombings Hit Atomic Experts in Iran Streets.” *The New York Times*, 29 November 2010. Accessed 12 February 2016, http://www.nytimes.com/2010/11/30/world/middleast/30tehran.html?_r=0.

Zetter, Kim. “Google Attack Was Ultra Sophisticated, New Details Show.” *Wired,* 14 January 2010. Accessed 7 September 2015. http://www.wired.com/2010/01/operation-aurora/.

Zetter, Kim, and Any Greenberg, “Why The OPM Breach is Such a Security and Privacy Debacle.” *Wired,* 11 June 2015. Accessed 7 September 2015. http://www.wired.com/2015/06/opm-breach-security-privacy-debacle/.

Papers/Reports

Anderson, Eric C., and Jeffrey G. Engstrom. "Capabilities of the Chinese People's Liberation Army to Carry Out Military Action in the Event of a Regional Military Conflict." East Asia Studies Center, Strategic Assessment Center, Advanced Analytics and Linguistics Division, Mission Integration Business Unit, Science Applications International Corporation Tysons Corner, VA, March 2009. Accessed 13 May 2016. http://origin.www.uscc.gov/sites/default/files/Research/CapabilitiesoftheChinesePeople'sLiberationArmytoCarryOutMilitaryActionintheEventofaRegionalConflict.pdf.

Appelgate, Scott D. "The Principles of Maneuver in Cyber Operations." 4th International Conference on Cyber Conflict. NATO CCD COE Publications, Tallin, 2012.

Booz Allen Hamilton. *Cyber Theft of Corporate Intellectual Property: The Nature of the Threat*. McLean, VA: Economist Intelligence Unit, Booz Allen Hamilton, 2012.

Caton, Jeffrey L. "Army Support of Military Cyberspace Operations: Joint Contexts and Global Escalation Implications" Monograph, Strategic Studies Institute, U.S. Army War College Press, Carlisle Barracks, PA, January 2015.

Chen, Thomas M. *An Assessment of the Department of Defense Strategy For Operations in Cyberspace*. The Letort Papers, Strategic Studies Institute, U.S. Army War College Press, Carlisle Barracks, PA, September 2013.

Cordesman, Anthony H., and Steven Colley. *Chinese Strategy and Military Modernization in 2015: A Comparative Analysis.* Washington, DC: Center for Strategic and International Studies, 10 October 2015.

Estonia. *Cyber Security Strategy*. Cyber Security Strategy Committee, Ministry of Defence, Tallinn, Estonia, 2008.

Falliere, Nicolas, Liam O. Murchu, and Eric Chien. *Symantec Security Response, W32.Stuxnet Dossier: Version 1.4.* Cupertino, CA: Symantec Corporation, February 2011.

Gomez, Alberto N. "Awaken the Cyber Dragon: China's Cyber Strategy and its Impact on ASEAN." The Second International Conference on Cyber Security, Cyber Peacefare and Digital Forensic (CyberSec2013). Kuala Lumpur, Malaysia, 2013.

Kao, John. "Silicon Valley: Metaphor for Cybersecurity, Key to Understanding Innovation War." In *Cyber Analogies*, edited by Emily O. Goldman and John Arquilla, 90-95. Technical Report, Naval Postgraduate School, Monterey, CA, 28 February 2014.

Krekel, Bryan. *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*. Prepared for The US-China Economic and Security Review Commission. Northrup Grumman, McLean, VA, 9 October 2009. *Northrop Grumman*.

Lieber, Kier. "The Offense-Defense Balance and Cyber Warfare." In *Cyber Analogies* edited by Emily O. Goldman and John Arquilla, 96-107. Technical Report, Naval Postgraduate School, Monterey, CA, 28 February 2014.

Malone, Patrick, J. "Offense Defense Balance in Cyberspace: A Proposed Model." Thesis, Naval Postgraduate, Monterey, CA, December 2012.

Mandiant. *APT 1: Exposing One of China's Cyber Espionage Units*. Intelligence Report. Mandiant, Milpitas, CA, 2013. Accessed 13 May 2016. http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

Phoenix Contact. "Hacking the Industrial Network." A White Paper, Phoenix Contact, Harrisburg, PA, undated.

Rodriguez, Stephen M. "USCYBERCOM: A Centralized Command of Cyberspace." Research Paper, Joint Military Operations Department, Naval War College, Newport, RI, 31 May 2011.

Theohary, Catherine, and John Rollins. *Cyberwarfare and Cyberterrorism: In Brief.* Washington, DC: Library of Congress, 27 March 2015.

Valerino, Brandon, and Ryan Maness. "A Theory of Cyber Espionage for the Intelligence Community." EMC Chair Conference Paper, U.S. Naval War College, Newport, RI, undated.

Wirtz, James J. "The Cyber Pearl Harbor." In *Cyber Analogies,* edited by Emily O. Goldman and John Arquilla, 7-14. Technical Report, Naval Postgraduate School, Monterey, CA, 28 February 2014.